



Last Updated Aug.15,2023

InstaShow™ White Paper

Network Deployment Guide for Integrating your InstaShow VS20
into your organization's network

v 1.00

Table of Contents

1	How to Use this White Paper	5
1.1	For Wireless Presentations	5
1.2	For Wireless Video Conferences	5
1.2.1	Network Connections and the InstaShow VS Assist App	5
2	Installing VS20 into your Network Configuration	6
2.1	Connecting InstaShow VS20 Using a Wired / Ethernet (RJ-45) Connection (Recommended)	6
2.2	Connecting InstaShow VS20 Using a Wireless Connection (Optional)	7
2.2.1	Limitations/Conditions for Connecting InstaShow VS20 Using a Wireless Connection	11
2.3	Direct Connections and In-Direct Connections to the InstaShow VS20 Host for Video Conferencing	12
2.4	Ensuring a Smooth Video Conference with Low Latency	13
2.4.1	Runtime Monitor Call Health for Microsoft Teams	14
2.4.2	Suggested Maximum Peak Wi-Fi Bandwidth at the Local Level for a Smooth InstaShow VS20 Experience	15
2.4.3	InstaShow VS20 Runtime Check for Wi-Fi Traffic Test	17
2.5	Wi-Fi Security Settings for Integrating InstaShow VS20 into your Organization's Network	21
3	Network Port and Firewall Settings	25
3.1	Network Port Requirements	25
3.2	Windows Defender Firewall Settings	26
3.3	Network Switch/Routers and Cross Networks in a Corporate Network	30
4	InstaShow VS Assist App Installation and Information	31
4.1	Hardware Requirements for the InstaShow VS Assist App on a Windows PC	31
4.2	Installing InstaShow VS Assist in a Corporate Environment	31

4.2.1	The Standard Full Installation Process	32
5	Video Conferencing	36
5.1	Supported Video Conferencing Peripherals and Setup Procedures	36
5.1.1	About the InstaShow VS20 Host's USB-A Ports	36
5.1.2	Connecting USB Peripherals to the InstaShow VS20 Host.....	37
5.1.3	Using the InstaShow VS Assist App to Check the Compatibility of Connected USB Peripherals.....	39
5.1.4	Using the Web Management Interface to Check the Compatibility of Connected USB Peripherals	41
5.1.5	Manually Selecting the Preferred Devices for a Specific USB-A Port	42
5.1.6	Supported Camera Input Resolution and Codec.....	45
5.1.7	Default Audio Output.....	46
5.2	Using InstaShow VS20 Buttons as Microphones.....	47
5.2.1	General Introduction.....	47
5.2.2	Using InstaShow VS20 as a Wireless Microphone System.....	48
5.2.3	Setting Up an Aggregated Wireless Microphone System with InstaShow VS20.....	51

List of Figures

Figure 1: Typical Wired (Ethernet) Connection	7
Figure 2: Typical Wireless (Repeater Mode) Connection	7
Figure 3: A video conference utilizing a direct connection to the VS20 Host	12
Figure 4: A video conference utilizing an indirect connection to the VS20 Host	13
Figure 5: Sample Wi-Fi Test Results.....	19
Figure 6: Laptop Wi-Fi Menu with Second SSID.....	24
Figure 7: Windows Security Alert for InstaShow VS Assist	27
Figure 8: Windows Security Alert for InstaShow VS Button	27
Figure 9: Windows Security Alert for InstaShow Local Display.....	27
Figure 10: Windows Security Alert for InstaShow VS RTSP	28
Figure 11: Windows Security Alert for InstaShow VS RTSP.....	28
Figure 12: Windows Firewall and Network Protection Menu.....	28
Figure 13: Windows Defender Firewall Allowed Apps	29
Figure 14: Windows Defender Firewall Advanced Security Menu.....	30
Figure 15: Windows Account Type for a Standard User	32
Figure 16: InstaShow VS20 Host's Rear USB-A Ports	36
Figure 17: Typical Wired (Ethernet) Connection.....	38
Figure 18: The InstaShow Camera Preview Button.....	40
Figure 19: Example Connected Devices Table	43
Figure 20: Example VC Devices in Use Table	44
Figure 21: Windows Device Manager with InstaShow VS20 Button Connected.....	47
Figure 22: InstaShow VS20 Button	48
Figure 24: Example Meeting Room.....	49
Figure 25: Device Suggestions from Logitech.....	51
Figure 26: Wireless Microphone Enabled in Web Management Interface.....	51
Figure 27: The TX Wi-Fi Microphone Field	52

List of Tables

Table 1: Suggested Maximum Peak Bandwidths for Basic Wireless Presentations	15
Table 2: Suggested Maximum Peak Bandwidths for Multi-User Presentations	16
Table 3: Suggested Maximum Peak Bandwidth for a Multi-Device Presentation...	16
Table 4: Suggested Maximum Peak Bandwidths for Video Conferencing.....	16
Table 5: Suggested Maximum Peak Bandwidth for Critical Scenarios	16
Table 6: Network Ports for VS20 Host and InstaShow VS Assist App	25
Table 7: Network Ports Used by Miracast and AirPlay	26
Table 8: Available USB-A Ports for InstaShow VS Series Models	36
Table 9: Order of Priority for USB-A Ports.....	36
Table 10: Example Device Connection Matrix.....	43
Table 11: Default Audio Output.....	47
Table 12: Recommended Microphone Deployment.....	49

1 How to Use this White Paper

1.1 For Wireless Presentations

To utilize InstaShow VS20's wireless presentation feature, you do not have to connect the InstaShow VS20 Host to a network or install any additional drivers or software. You only need to connect the HDMI output port on the Host to your conference room's display or projector to be able to use InstaShow VS20's plug and play Button to wirelessly project your presentation file onto the display/projector.

1.2 For Wireless Video Conferences

InstaShow VS20 supports all mainstream USB-A video conferencing peripherals (webcams, microphones, speakers, etc.) which can be connected to the InstaShow VS20 Host's USB-A 3.0 port for use. Once you have installed the InstaShow VS Assist app onto your local PC and connected it to your organization's network, you will be able to access the connected peripherals via Microsoft Teams or any other video conferencing application.

1.2.1 Network Connections and the InstaShow VS Assist App

Before using InstaShow VS20 in a wireless video conference, you should first check to see if your organization's network connection is stable and that your organization's IT policy permits the use of both the InstaShow VS20 Host and the InstaShow VS Assist app.

To ensure that a wireless video conference with InstaShow VS20 proceeds smoothly without any issues, you can refer to the following cross-references:

- For recommendations for connecting the InstaShow VS20 Host to a wired network via an RJ45 cable, see [Connecting InstaShow VS20 Using a Wired / Ethernet \(RJ-45\) Connection \(Recommended\)](#) on page 6.
- For recommendations for connecting your local (host) PC to the InstaShow VS20 Host, see [Direct Connections and In-Direct Connections to the InstaShow VS20 Host for Video Conferencing](#) on page 12.
- For further instructions on setting up your company network to allow for InstaShow VS20's full wireless video conferencing features (due to your organization's IT policy), see [Network Port and Firewall Settings](#) on page 25.
- For more information on using USB 2.0 3-in-1 video conferencing peripherals with InstaShow VS20, see [Video Conferencing](#) on page 36.

2 Installing VS20 into your Network Configuration

The InstaShow VS20 Host (receiver) can connect to your organization's network using one of the following methods:

- Wired connection via an Ethernet (RJ-45) cable
- Wireless connection via the "Repeater mode" option in InstaShow VS20's settings menu

Before you begin, first make sure that (1) the InstaShow VS20 Host is permitted in your network¹, (2) the network ports used by both the InstaShow VS20 Host and the InstaShow VS Assist app are allowed access to your network. For more information on configuring your network ports, see the Network Port and Firewall Settings section on page 25.

Security Mode: By default, each InstaShow VS20 Host broadcasts a single SSID for wireless connections by laptops and mobile devices. Each Host also features the capacity to create WPA2 Enterprise SSID to separate Guest LAN and Corporate LAN. For detail setup, see [Wi-Fi Security Settings](#)

2.1 Connecting InstaShow VS20 Using a Wired / Ethernet (RJ-45) Connection (Recommended)

A wired connection via an Ethernet cable is the recommended method for connecting the InstaShow VS20 Host to your network. Once the Host is integrated into the network, connecting all laptops and mobile devices to the InstaShow Host directly when presenting is also recommended.

¹ Depending on your organization's IT policy, your InstaShow's MAC address may be blocked from your organization's network. As a result, if you fail to connect your VS20 Host to the network, check with your IT staff to get network access permission.

The figure below shows how to setup a typical wired connection.

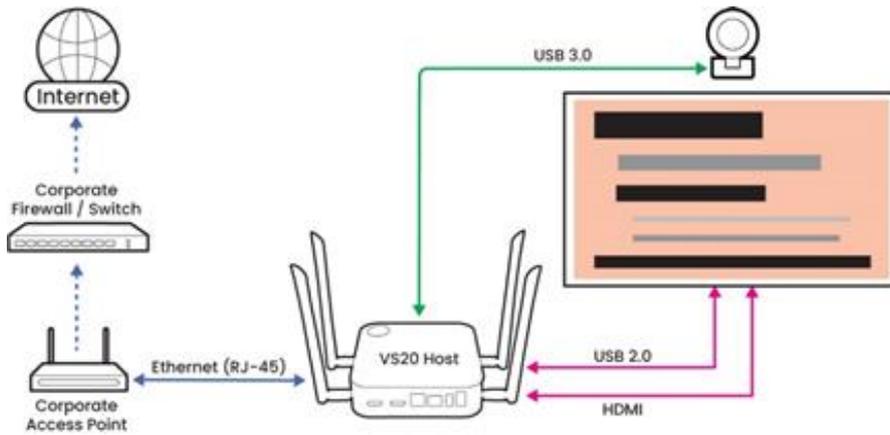


Figure 1: Typical Wired (Ethernet) Connection

2.2 Connecting InstaShow VS20 Using a Wireless Connection (Optional)

The other method for connecting the InstaShow VS20 Host to your network is to connect it wirelessly to your organization's wireless access point (a wired connection is the recommended connection method). Connecting the Host to your network wirelessly must be done via InstaShow VS20's Wireless Repeater feature.

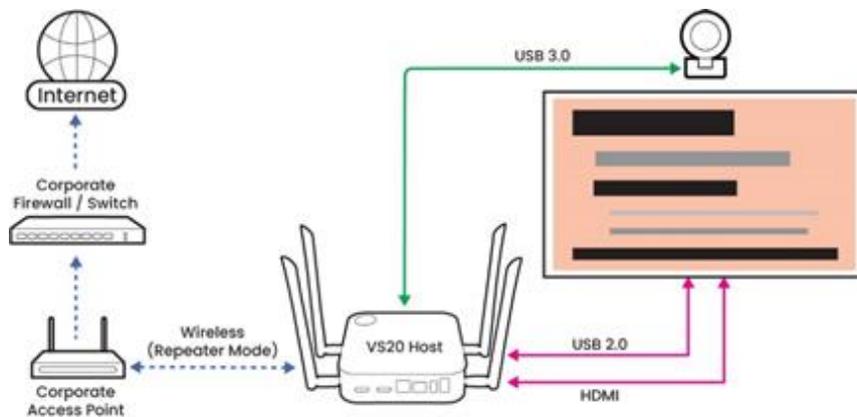
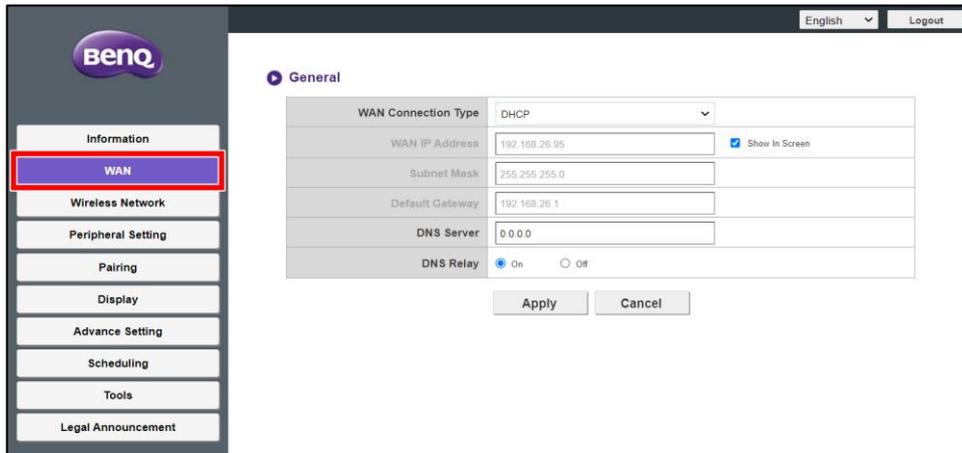


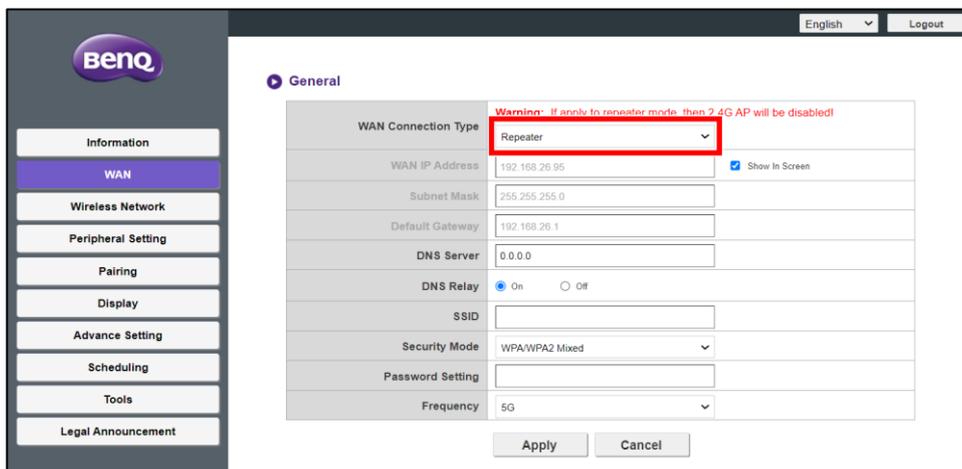
Figure 2: Typical Wireless (Repeater Mode) Connection

To connect the InstaShow VS20 Host to your organization's wireless access point via the Wireless Repeater feature:

1. Log into the InstaShow VS20 Host's Web Manager interface.²
2. Enter the **WAN** menu.



3. In the **WAN Connection Type** field, select **Repeater**.



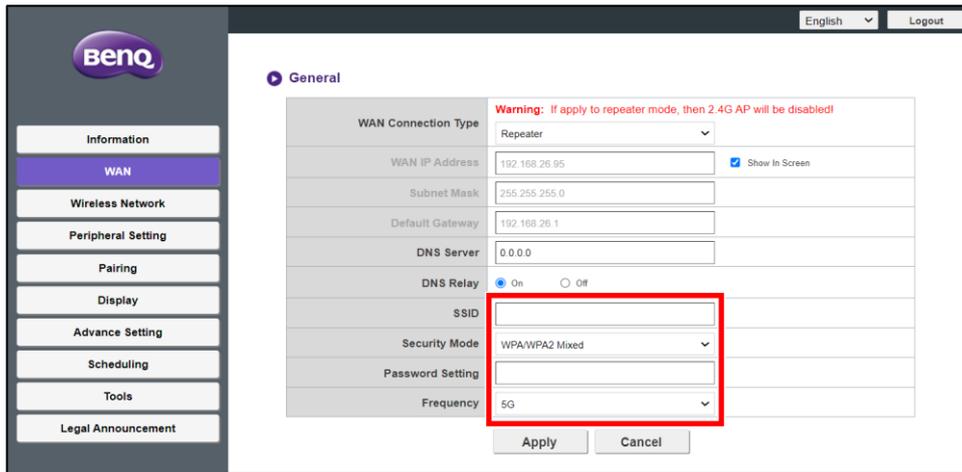
4. In the **SSID** and **Password Setting** fields, enter the SSID and password of the wireless access point you want to connect the Host to respectively.

*NOTE 1: The **SSID** and **Password Settings** fields have the following input criteria: (1) limit of no less than 8 and no more than 32 characters only, (2) support for numerals, lower-case and upper-case letters, periods (.), dashes (-), underscores (_), and at signs (@) only.*

NOTE 2: Repeater mode only supports a 5G signal, once enabled the Host's 2.4G signal will be disabled.

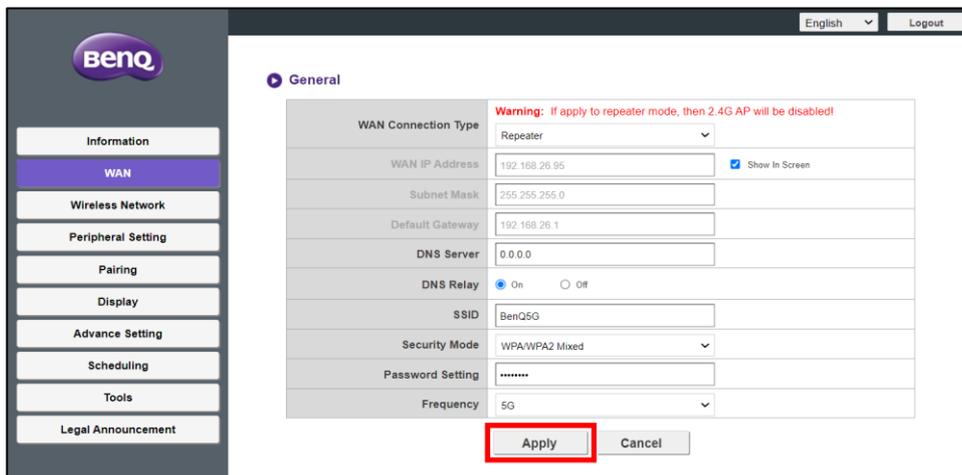
NOTE 3: Repeater mode only supports WPA/WPA Mixed security encryption. WPA-Enterprise is not supported.

² Refer to the VS20 User Manual for instructions on logging into the Web Management interface.



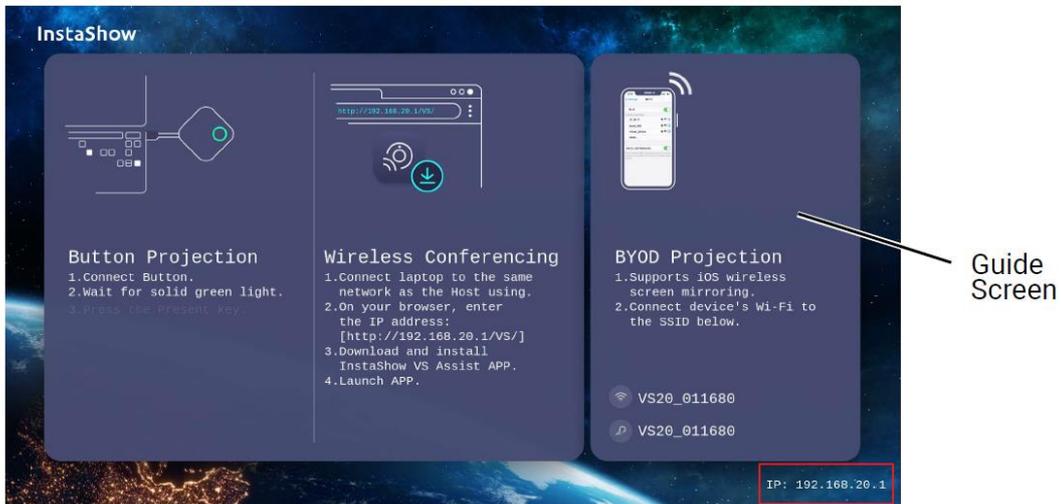
5. Click **Apply** for Repeater mode to take effect, the Host will automatically reboot itself and connect to the wireless access point.

NOTE: In the image below the SSID "BenQ5G" is only used as an example. Use the actual SSID for your organization's wireless access point when connecting.



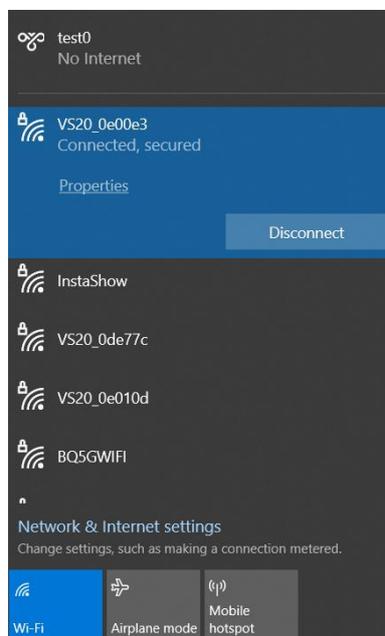
- Once the Host has connected to the wireless access point, the IP address shown on the VS20 guide screen will switch from the default IP address (192.168.20.1) to the IP address for your organization's network.

NOTE: You can use Windows Command Prompt to find your organization's IP address. See <https://networking.grok.lsu.edu/article.aspx?articleid=14842&printable=y> for instructions.



- Connect your system (e.g., laptop, mobile device) to the Host's Wi-Fi SSID (i.e., NOT the wireless access point's SSID).

NOTE: In the image below the SSID "V20_0e00e3" is used as an example of the SSID for an InstaShow VS20 Host's Wi-Fi signal.



In repeater mode, the InstaShow VS20 Host acts as a Wi-Fi signal repeater where one of its Wi-Fi channels is connected to the organization's wireless access point while the other channel stays as a wireless access point for other devices to connect to. As such, once a device is connected to the Host's Wi-Fi signal, the Host will forward all incoming and outgoing traffic to the organization's wireless access point.

2.2.1 Limitations/Conditions for Connecting InstaShow VS20 Using a Wireless Connection

When using InstaShow VS20's Repeater mode to connect to your organization's wireless network, the following limitations/conditions will apply:

- When set to Repeater mode, the InstaShow VS20 Host's wireless bandwidth will be halved³. As a result, a wired connection is highly recommended as the first choice for connecting the Host to your organization's network while a wireless connection via Repeater mode should only be used when the setting is not suitable for a wired connection.
- If the wireless access point that the InstaShow VS20 is connecting to via Repeater mode supports both the 2.4 GHz and 5 GHz frequency bands, the InstaShow VS20 will only be able to connect to one of the bands when using Repeater mode.
- The bandwidth for the InstaShow VS20 Host must be the same as the bandwidth for the wireless access point it is connected to. So, for example if the bandwidth for the access point is 80MHz, and the bandwidth for the Host is 40Mhz, then it is recommended to set the bandwidth of the access point to 40MHz (to match the Host) in order to diminish compatibility problems when connecting.
- The channels used by both the InstaShow VS20 Host and wireless access point must be the same. So, if for example your wireless access point is set to channel 100 (DFS Channel) in the US, because InstaShow VS20 does not support DFS in US, the wireless access point must be switched to band 1 (CH36, CH40, CH44, CH48) or band 4 (CH149, CH153, CH157, CH161, CH163).
- The performance of the InstaShow VS20 Host's connection with your organizations wireless network will be affect by the wireless environment.

³ <https://geekabit.co.uk/2018/01/21/wireless-repeaters-the-disadvantages/>

2.3 Direct Connections and In-Direct Connections to the InstaShow VS20 Host for Video Conferencing

When using InstaShow VS20 in video conferencing scenarios, the user will have to install the InstaShow VS Assist app into at least one Windows PC⁴ that will then act as the system hosting the video conference.

There are two ways to connect the system running the InstaShow VS Assist app to the InstaShow VS20 Host and proceed with the video conference:

- A direct connection in which the PC hosting the video conference (in the meeting room) will connect to the InstaShow VS Host via its Wi-Fi signal and then log into in the video conference app.

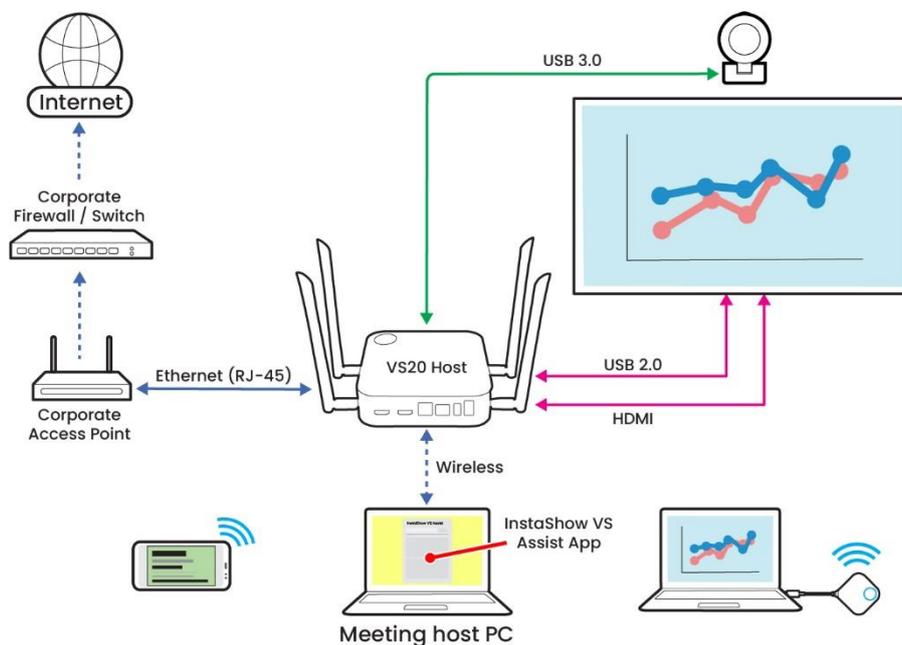


Figure 3: A video conference utilizing a direct connection to the VS20 Host

⁴ As of now the InstaShow VS Assist app is only available for Windows.

- An indirect connection in which the devices connect to the organization’s wireless access point through which all the traffic goes through.

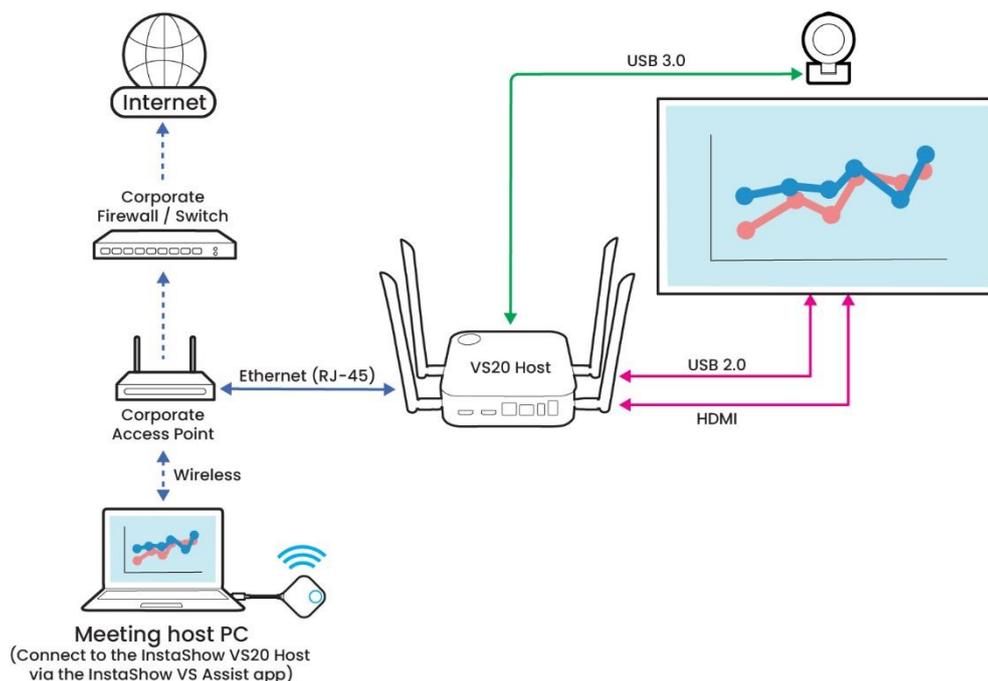


Figure 4: A video conference utilizing an indirect connection to the VS20 Host

NOTE 1: Normally networks within an organization will set different subnets via switch VLAN segmentation in order to serve all its employees/staff. Based on the organization’s IT policy, when Internet is not allowed, use [an indirect connection](#) (Figure 4) to set the InstaShow VS20 Host and devices to the same Intranet network. The user can then check the IP address from the InstaShow guide screen. The WAN IP address may differ from the IP address of your PC/laptop. To check the IP address of your PC/laptop please type “ipconfig” in Windows Command Prompt and all IP addresses for your laptop will be listed.

NOTE 2: Network bandwidth efficiency needs to be considered when using the InstaShow VS Assist app with an indirect connection. To support video conferencing certain bandwidth needs to be allocated to the host PC for the meeting, but given that the network’s total bandwidth is shared by all employees, video conferencing via an indirect connection may not guarantee a smooth experience throughout the meeting.

2.4 Ensuring a Smooth Video Conference with Low Latency

A successful video conference with InstaShow VS20 that incorporates video, audio, and screensharing entails that you ensure the following items are accounted for:

- A Wi-Fi connection between the host PC in the meeting (i.e., the device that is accessing the InstaShow Host and its connected peripherals) and the InstaShow VS20 Host that is consistent and of a sufficient speed.
- A strong Internet connection for the device(s) used by each participant, both local and remote.
- A strong and steady connection used by the video conferencing application for each participant, both local and remote.

To learn how to optimize the Wi-Fi connection between each local device and the InstaShow VS Host, see the Suggested Maximum Peak Wi-Fi Bandwidth at the Local Level for a Smooth InstaShow VS20 Experience section on page [錯誤! 尚未定義書籤](#).

To test/check the Internet connection for each participating device, you can use any commonly-used speed test websites or tools. The quality of the Internet connection will depend on the telecom service used by the device and *not* the InstaShow VS20 Host.

To optimize the network performance for your video conferencing application, refer to the support information provided by your respective video conferencing service. For Microsoft Teams users, Microsoft provides instructions on how to optimize Teams' video conferencing including an additional network assessment tool for Microsoft 365 users.⁵

2.4.1 Runtime Monitor Call Health for Microsoft Teams

Microsoft Teams also features a runtime call health status tool called "Call Health". This tool is able to monitor the network, audio, video (camera), and screensharing status for each specific device participating in a Teams meeting and, based on calculations by its AI, is able to adjust and compress the audio, video, and screensharing accordingly.⁶ This allows Teams to ensure that the video conference runs smoothly. For more information on this tool click the following link:

<https://support.microsoft.com/en-us/office/monitor-call-and-meeting-quality-in-teams-7bb1747c-d91a-4fbb-84f6-ad3f48e73511>.

⁵ <https://learn.microsoft.com/en-us/microsoftteams/business-voice/get-ready-internet>

⁶ In instances where network performance is poor, Teams will prioritize the audio signal over video and screensharing to keep every participant engaged.

2.4.2 Suggested Maximum Peak Wi-Fi Bandwidth at the Local Level for a Smooth InstaShow VS20 Experience

InstaShow VS20 acts as a Wireless Presentation System (WPS) with the same user experience as BenQ’s InstaShow WDC series, with improvements this time around that have increased the maximum supported resolution to 4K30 for Button to Host connections.⁷

In terms of ensuring that the WPS aspect of InstaShow VS20’s functionality runs smoothly, focus should be paid on the quality of the connection between the presenting devices (InstaShow Buttons, mobile devices, and laptops) and the InstaShow VS20 Host. As such, mentions of bandwidth in the discussion below refers to the data transmission between the devices and Host.

The tables below detail the suggested maximum peak bandwidth for various scenarios to ensure a smooth InstaShow VS20 experience. These are suggested maximum peak bandwidths only that IT can refer to while using a floor plan. The real consumed bandwidth will depend on the complexity of the content. Normally the consumed bandwidth is lower than the maximum peak bandwidth.

For Basic Wireless Presentations

Scenario	Resolution	Suggested Max. Peak Bandwidth
One Button	1080p60	8 Mbps
One Button	4K30	12 Mbps
One Mobile Device (via AirPlay)	1080p60	25 Mbps (as recommended by Apple)
One Mobile Device (via Miracast)	1080p60	20 Mbps (based on real tests)

Table 1: Suggested Maximum Peak Bandwidths for Basic Wireless Presentations

For Multi-User Simultaneous Presentations via the Split-Screen Feature⁸

Scenario	Resolution	Suggested Max. Peak Bandwidth
----------	------------	-------------------------------

⁷ For laptops in general, only when a 2nd screen is set to “Extend” can its resolution reach 4K30, otherwise when set to “Duplicate” the 2nd screen’s resolution will be limited to the laptop’s built-in display’s resolution.

⁸ When there are 2 or more devices projecting their screens simultaneously, the 4K30 max resolution will be scaled down to 1080p60.

One Button	4K30	12 Mbps
Two Buttons	1080p60 per Button	16 Mbps
Three Buttons	1080p60 per Button	24 Mbps
Four Buttons	1080p60 per Button	32 Mbps

Table 2: Suggested Maximum Peak Bandwidths for Multi-User Presentations

For Multi-User Presentations Involving Buttons and Mobile Devices/Laptops

Scenario	Suggested Max. Peak Bandwidth
Two Buttons + One AirPlay Device + One Miracast Device	61 Mbps

Table 3: Suggested Maximum Peak Bandwidth for a Multi-Device Presentation

For Video Conferencing

Scenario	Suggested Max. Peak Bandwidth
Audio Only (Speaker and Microphone)	1 Mbps
Video Only (Webcam)	23 Mbps
Audio + Video	24 Mbps
InstaShow Display Sharing (Per Sharer)	5 Mbps
Audio + Video + InstaShow Display Sharing	30 Mbps

Table 4: Suggested Maximum Peak Bandwidths for Video Conferencing

For Critical Scenarios

The information shown below is the full bandwidth needed to ensure a smooth experience under a critical scenario (i.e., wireless presentation with a full array of devices *and* video conferencing), but because most uses of InstaShow VS20 are not in a critical scenario, the full bandwidth may not be needed.

Scenario	Suggested Max. Peak Bandwidth
Wireless Presentation (Two Buttons + One AirPlay Device + One Miracast Device) + Video Conferencing (Audio + Video) + InstaShow Display Sharing	91 Mbps

Table 5: Suggested Maximum Peak Bandwidth for Critical Scenarios

NOTE: The suggested maximum peak bandwidth can be applied to both Wi-Fi and wired networks in a corporate environment.

2.4.3 InstaShow VS20 Runtime Check for Wi-Fi Traffic Test

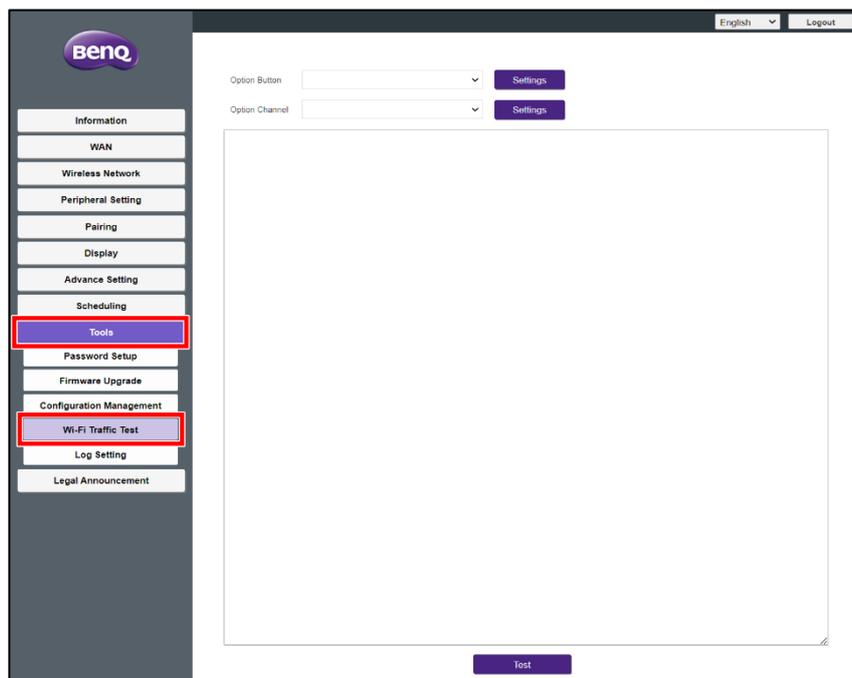
The user can utilize the following tools to check the quality of the wireless meeting. They can be split into 2 separate sections: the first is a test of the wireless presentation system's bandwidth for transmission and delivery, the second is a check of how much of the PC's resources are dedicated to the InstaShow VS Assist app during use.

Bandwidth (Transmission & Delivery) Test

As with the InstaShow WDC20 and WDC30, InstaShow VS20 also features a built-in Wi-Fi Traffic Test tool that allows IT staff and System Integrators (SI) to check their Wi-Fi environment before deploying InstaShow VS20 for use. It is suggested that the Wi-Fi Traffic Test is used along with the Channel Deployment Plan before deploying VS20.

To use the Wi-Fi Traffic Test tool to test your Wi-Fi environment:

1. Log into the Host's Web Management interface.⁹
2. Enter the **Tool > Wi-Fi Traffic Test** menu.

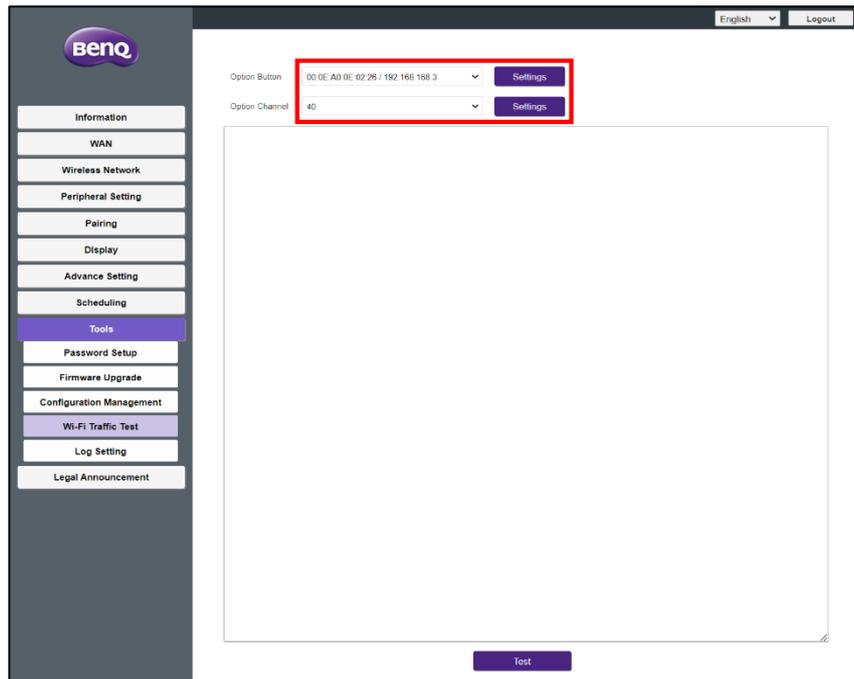


3. In the **Option Button** field, select the InstaShow VS20 Button that is connected to the InstaShow VS20 Host and then click **Settings** to set the corresponding Button for the test.

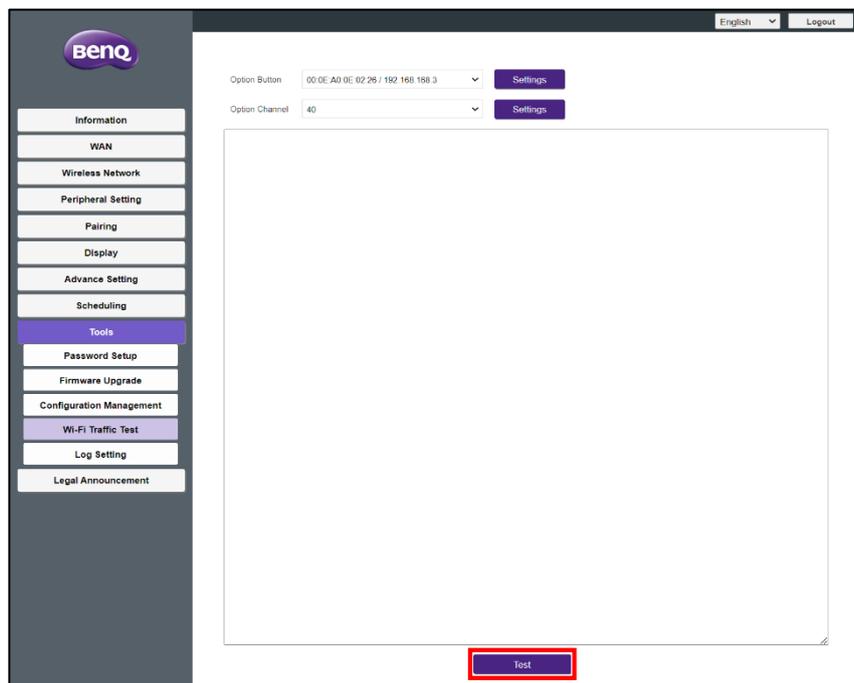
NOTE: The distance between the Button and Host will affect the result.

⁹ Refer to the VS20 User Manual for instructions on logging into the Web Management interface.

4. In the **Option Channel** field, select the Wi-Fi channel which you want your Host to utilize and then click **Settings** to set the corresponding Wi-Fi channel for the test.



5. Click **Test**. The test will run for approximately 90 seconds after which the results will appear.



The example below shows the results of a Wi-Fi Traffic Test for a Wi-Fi Channel of 40 (DFS Enabled¹⁰). The results show good Wi-Fi bandwidth for the setting in which the test was conducted, with speeds consistently over 100 Mbps. The speed however drops to 49.7 Mbps in the 70 – 71 second range, which means that if you use InstaShow VS20 to wirelessly present *and* video conference in a critical scenario (similar to the one described earlier), you may encounter lag in the video and audio, while most other presentation or video conferencing sessions will work fine.

NOTE: Make sure you have consistent throughput via the Wi-Fi traffic test.

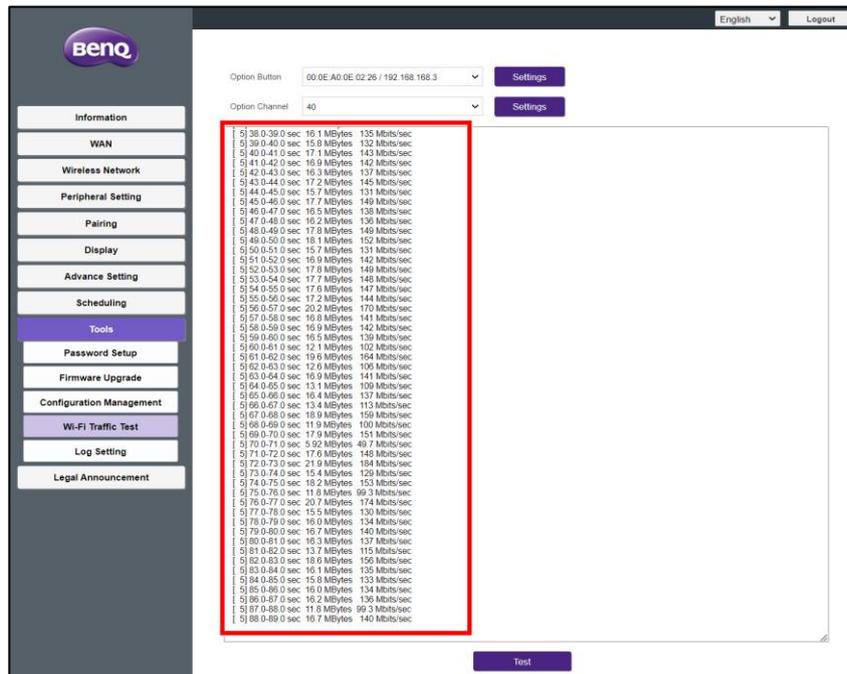


Figure 5: Sample Wi-Fi Test Results

InstaShow VS Assist App Usage Test

Once you have begun a video conference via the InstaShow VS Assist app, the performance of the meeting's host PC's resources will also affect the quality of the video conference. Follow the steps below to test its performance:

1. On the host PC, open Windows Control Panel.
2. Select **System** to view the system information.

¹⁰ DFS channels are only available in certain countries. Check with our sales department for availability.

3. Launch the InstaShow VS Assist app and connect to the InstaShow VS20 Host.
 4. Launch your corresponding video conferencing application.
- NOTE: Microsoft Teams is used in the examples below.*
5. In the InstaShow VS Assist app select **InstaShow Camera** and **InstaShow Audio** for the video conferencing microphone and speaker respectively.
 6. Join the video conferencing meeting/session.
 7. In the InstaShow VS Assist app, open **InstaShow Display Sharing**.
 8. Click the screen sharing function in the video conferencing application and select the InstaShow Display Sharing window.
 9. Open Windows Task Manager and check the status of the resources (including network).

The screenshot shows the Windows Task Manager Performance tab. The top bar indicates overall system usage: 17% CPU, 84% Memory, 1% Disk, and 0% Network. Below this, a table lists the resource usage for 11 applications. The 'InstaShow VS Assist' application is highlighted in grey.

Name	Status	17% CPU	84% Memory	1% Disk	0% Network
Apps (11)					
> Google Chrome (10)		0%	500.4 MB	0.1 MB/s	0 Mbps
> InstaShow VS Assist		0%	3.5 MB	0.1 MB/s	0 Mbps
> Microsoft Edge (8)		0%	64.0 MB	0 MB/s	0 Mbps
> Microsoft Excel (9)		0%	34.8 MB	0 MB/s	0 Mbps
> Microsoft Outlook (9)		0.9%	166.3 MB	0 MB/s	0.1 Mbps
> Microsoft Teams (5)		0%	173.0 MB	0.1 MB/s	0 Mbps
> Microsoft Word (3)		0.6%	201.7 MB	0 MB/s	0 Mbps

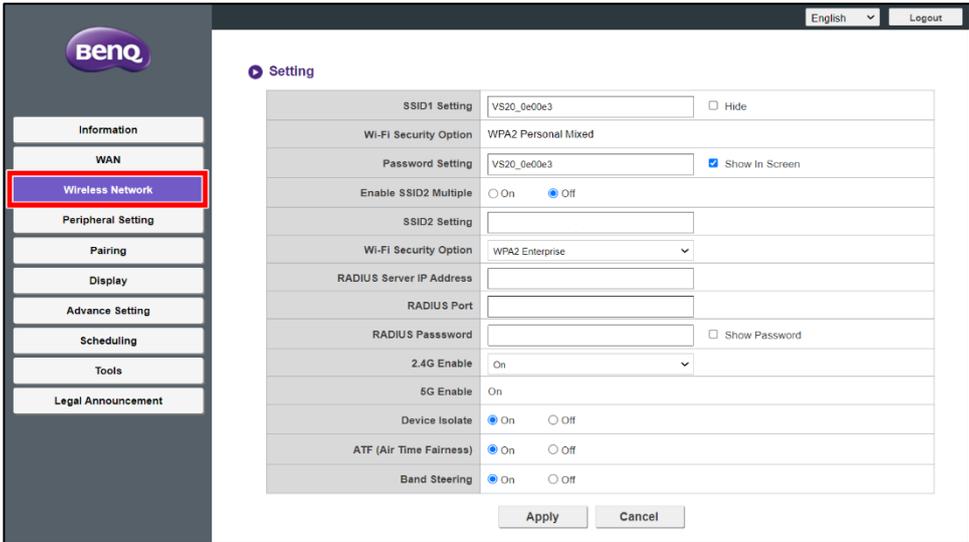
In the example above, the bandwidth consumed by the Microsoft Teams meeting is around 21 Mbps in total and less than the suggested maximum peak bandwidth outlined earlier.

2.5 Wi-Fi Security Settings for Integrating InstaShow VS20 into your Organization's Network

By default, each InstaShow VS20 Host broadcasts a single SSID for wireless connections by laptops and mobile devices, but given the need for organizations to provide separate access to different groups of users (such as guests or employees) for security reasons, each Host also features the capacity to create multiple SSIDs. Each SSID then represents a separate wireless network that users can connect to while sharing the same underlying physical network infrastructure. With multiple SSIDs, a single access point can provide network access to different groups of users or devices with varying levels of network access and security.

To enable your InstaShow VS20 Host to create multiple SSIDs:

1. Log into the Host's Web Management interface.¹¹
2. Enter the **Wireless Network** menu.



The screenshot displays the BenQ Web Management interface. On the left is a navigation menu with the BenQ logo at the top and several menu items: Information, WAN, Wireless Network (highlighted with a red box), Peripheral Setting, Pairing, Display, Advance Setting, Scheduling, Tools, and Legal Announcement. The main content area is titled 'Setting' and contains a table of configuration options:

SSID1 Setting	VS20_0e00e3	<input type="checkbox"/> Hide
Wi-Fi Security Option	WPA2 Personal Mixed	
Password Setting	VS20_0e00e3	<input checked="" type="checkbox"/> Show In Screen
Enable SSID2 Multiple	<input type="radio"/> On <input checked="" type="radio"/> Off	
SSID2 Setting		
Wi-Fi Security Option	WPA2 Enterprise	
RADIUS Server IP Address		
RADIUS Port		
RADIUS Password	<input type="checkbox"/> Show Password	
2.4G Enable	On	
5G Enable	On	
Device Isolate	<input checked="" type="radio"/> On <input type="radio"/> Off	
ATF (Air Time Fairness)	<input checked="" type="radio"/> On <input type="radio"/> Off	
Band Steering	<input checked="" type="radio"/> On <input type="radio"/> Off	

At the bottom of the settings table are two buttons: 'Apply' and 'Cancel'.

¹¹ Refer to the VS20 User Manual for instructions on logging into the Web Management interface.

3. In the **Enable SSID2 Multiple** field, select **On**.

The screenshot shows the BenQ wireless network settings interface. On the left is a navigation menu with categories: Information, WAN, Wireless Network (highlighted), Peripheral Setting, Pairing, Display, Advance Setting, Scheduling, Tools, and Legal Announcement. The main area is titled 'Setting' and contains a list of configuration fields. The 'Enable SSID2 Multiple' field is highlighted with a red box, showing the 'On' radio button selected. Other fields include SSID1 Setting (VS20_0e00e3), Wi-Fi Security Option (WPA2 Personal Mixed), Password Setting (VS20_0e00e3), SSID2 Setting (VS20_0e00e3_Laptop), Wi-Fi Security Option (WPA2 Enterprise), RADIUS Server IP Address, RADIUS Port, RADIUS Password, 2.4G Enable (On), 5G Enable (On), Device Isolate (On), ATF (Air Time Fairness) (On), and Band Steering (On). 'Apply' and 'Cancel' buttons are at the bottom.

4. In the **SSID2 Setting** field, enter the name you want to use for the second SSID.
5. In the **Wi-Fi Security Option** field, select the type of Wi-Fi security setting you want for the second SSID.

*NOTE: The **Wi-Fi Security Option** field for the original SSID1 is fixed at WPA2 Personal Mixed and is not adjustable.*

This screenshot is similar to the previous one, showing the same BenQ wireless network settings page. In this view, the 'SSID2 Setting' and 'Wi-Fi Security Option' fields are highlighted with a red box. The 'SSID2 Setting' field contains the text 'VS20_0e00e3_Laptop' and the 'Wi-Fi Security Option' dropdown menu is set to 'WPA2 Enterprise'. All other fields and the overall layout remain the same as in the previous screenshot.

6. In the **RADIUS Server IP Address** and **RADIUS Port** fields enter the corresponding information for your organization's network.¹²

The screenshot shows the BenQ wireless network settings page. The left sidebar contains a menu with options: Information, WAN, Wireless Network (selected), Peripheral Setting, Pairing, Display, Advance Setting, Scheduling, Tools, and Legal Announcement. The main content area is titled 'Setting' and contains various configuration options. The 'RADIUS Server IP Address' and 'RADIUS Port' fields are highlighted with a red box. The IP address is '0.0.0.0' and the port is '1812'. Other settings include SSID1 Setting (VS20_0e00e3), Wi-Fi Security Option (WPA2 Personal Mixed), Password Setting (VS20_0e00e3), Enable SSID2 Multiple (On), SSID2 Setting (VS20_0e00e3_Laptop), Wi-Fi Security Option (WPA2 Enterprise), RADIUS Password, 2.4G Enable (On), 5G Enable (On), Device Isolate (On), ATF (Air Time Fairness) (On), and Band Steering (On). There are 'Apply' and 'Cancel' buttons at the bottom.

7. Click **Apply** to save the settings.

The screenshot shows the BenQ wireless network settings page, identical to the previous one. The 'Apply' button at the bottom is highlighted with a red box.

¹² For certain organizations, integrating a RADIUS server into an AD server allows for centralized management of the authentication and authorization procedure for users who access network resources, including wireless access points, VPNs, and other remote access technologies. When a user attempts to access the organization's network resources, the RADIUS server communicates with the AD server to authenticate the user's credentials and check their authorization before allowing them access. The integration of RADIUS and AD simplifies the management of network access control, as it eliminates the need to manage separate user accounts and credentials for different network resources. It also provides a more secure method of authentication and authorization, as user credentials are stored in a central location and can be managed using the AD's robust access control policies.

When the multiple SSID feature is enabled, the idle screen for InstaShow VS20 will only display the original SSID. The second SSID can only be seen from the Wi-Fi menu of any laptops and/or mobile devices within the InstaShow VS20 Host's Wi-Fi signal range, as seen in the image below.



Figure 6: Laptop Wi-Fi Menu with Second SSID

3 Network Port and Firewall Settings

Before connecting InstaShow VS20 Host to your organization’s network you may need to make sure that the network ports used by both the Host and the InstaShow VS Assist app are allowed access. This chapter will explain the requirements for network port and firewall settings which IT staff can use to properly set up InstaShow VS20.

3.1 Network Port Requirements

The InstaShow VS20 Host and InstaShow VS Assist app communicate via standard TCP/IP network protocols. Since network ports and applications that generate network traffic may be blocked from your organization’s network by its firewall policies, certain network ports must be enabled in the devices within the network infrastructure (e.g., network switches, wireless routers, laptops) before you can properly set up InstaShow VS20.

Network Ports Used by the InstaShow VS20 Host and InstaShow VS Assist App

Application	Port	Function
InstaShow VS20 Host and InstaShow VS Assist App	18554 (TCP) 28554 (TCP) 38554 (TCP) 48556 (TCP) 58554 (TCP) 402 – 409 (TCP) 4010 – 4033 (TCP) 40100 – 40131 (TCP)	Video Streaming
InstaShow VS20 Host and InstaShow VS Assist App	18555 (UDP) 18553 (TCP) 28553 (TCP) 38553 (TCP)	Audio Streaming
InstaShow VS20 Host and InstaShow VS Assist App	1900 (UDP) 7000 (UDP)	Communication Data
InstaShow VS20 Host	80 (TCP) 443 (TCP)	Checking the BenQ Server
InstaShow VS Assist App		OTA Updates from the BenQ Server

Table 6: Network Ports for VS20 Host and InstaShow VS Assist App

Network Ports Used by Miracast and AirPlay

Application	Port	Use
Miracast	7236 (TCP)	Wi-Fi Direct Control Port
Miracast	7250 (TCP)	Miracast Packets Port
Miracast	48689 (UDP)	Miracast Broadcast Protocol
AirPlay	6000 – 7000 (TCP) 7100 (TCP) 47000 (TCP) 47010 (TCP)	AirPlay Traffic
AirPlay	5353 (UDP)	Bonjour Discovery
AirPlay	6000 – 7000 (UDP) 7011 (UDP)	AirPlay Traffic

Table 7: Network Ports Used by Miracast and AirPlay

3.2 Windows Defender Firewall Settings

Windows Defender Firewall is a software firewall built into the Windows operating systems. It provides protection by monitoring and controlling incoming and outgoing network traffic based on predefined security rules. Windows Defender Firewall allows you to block or allow network traffic for specific applications or services running on your computer. It also helps to protect your computer from unauthorized access and malicious attacks by filtering out potentially harmful traffic.

By default, Windows Defender Firewall is enabled on all Windows operating systems to provide a basic level of protection against network-based attacks. However, it is recommended that Windows users supplement this protection with additional security measures such as anti-virus software, regular software updates, and safe browsing practices.

The InstaShow VS Assist app registers several applications into Windows Defender Firewall which can be monitored by Windows. **Windows Security Alert** pop-ups will appear during the installation process and the initial launch of the InstaShow VS Assist app. **Windows Security Alert** pop-ups are notifications that appears on screen when Windows Defender Firewall or other security features detect a potential security threat.

The figures below show the pop-ups that appear during the initial launch of the InstaShow VS Assist app, these are due to the automatic generation of registry keys in Windows. The registry is used to store the firewall rules for each application which the firewall uses to determine whether to allow or block network traffic for that application. You will not need to worry about these **Windows Security Alert** pop-ups when launching the InstaShow VS Assist app for the first time.

*NOTE: Clicking **Cancel** will not affect the app when it is used to join a video conference.*

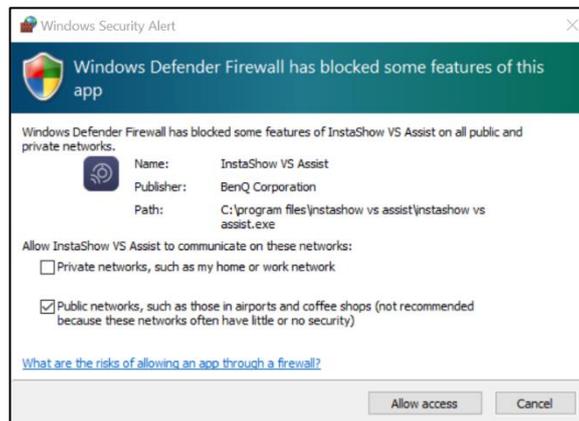


Figure 7: Windows Security Alert for InstaShow VS Assist

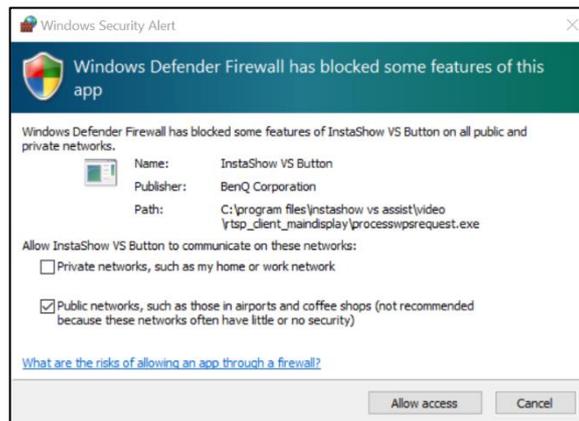


Figure 8: Windows Security Alert for InstaShow VS Button

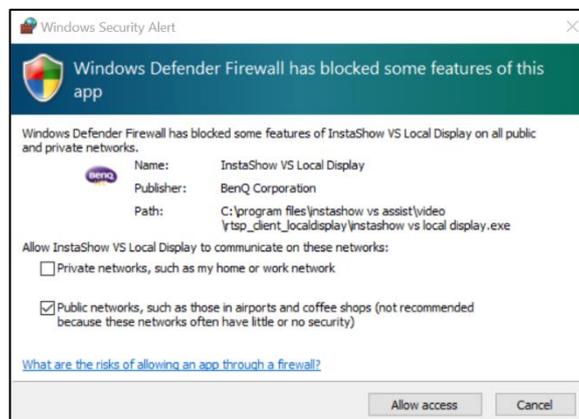


Figure 9: Windows Security Alert for InstaShow Local Display

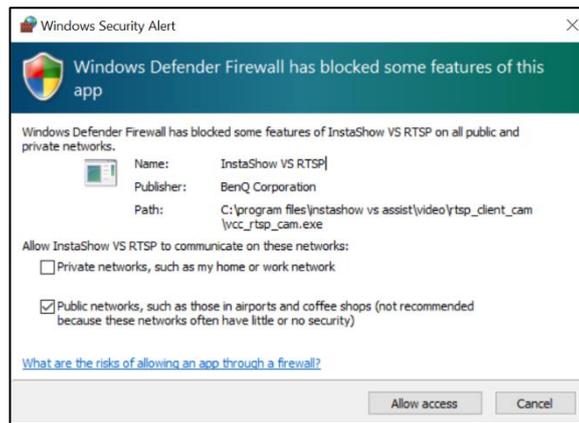


Figure 10: Windows Security Alert for InstaShow VS RTSP

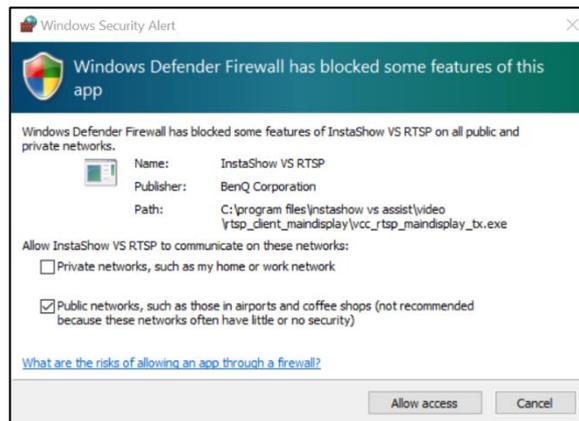


Figure 11: Windows Security Alert for InstaShow VS RTSP

For more detailed information, open **Firewall and network protection** in the Windows system settings menu and select **Allow an app through firewall** to check the status of the application firewalls, as seen in the figure below.

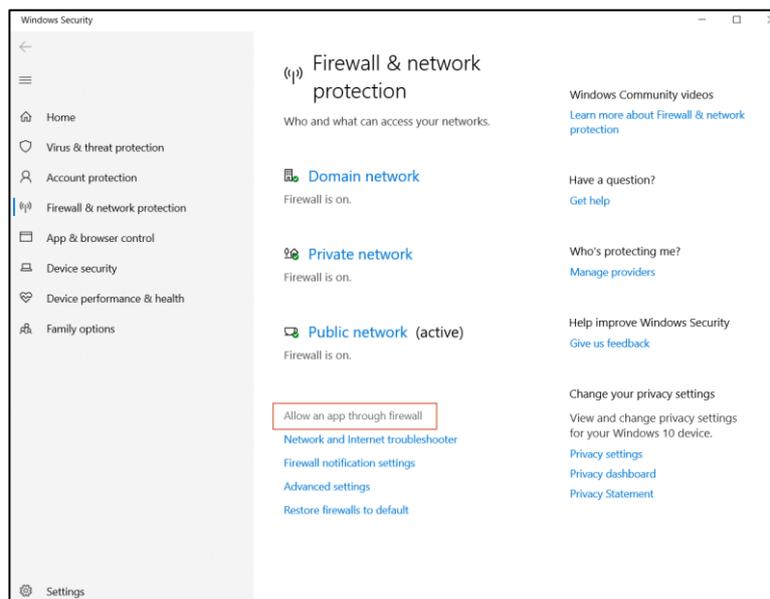


Figure 12: Windows Firewall and Network Protection Menu

Applications related to **InstaShow VS Assist** are not allowed by Windows which will not affect the InstaShow VS Assist's video conferencing features. Below is the list of applications related to InstaShow VS Assist which are registered but not allowed:

- InstaShow VS Assist
- InstaShow VS Button
- InstaShow VS Local Display
- InstaShow VS RTSP (for TCP)
- InstaShow VS RTSP (for UDP)

The inbound ports used by these applications are blocked by Windows Defender Firewall, as seen in the figures below, which allows IT staff more network policy flexibility.

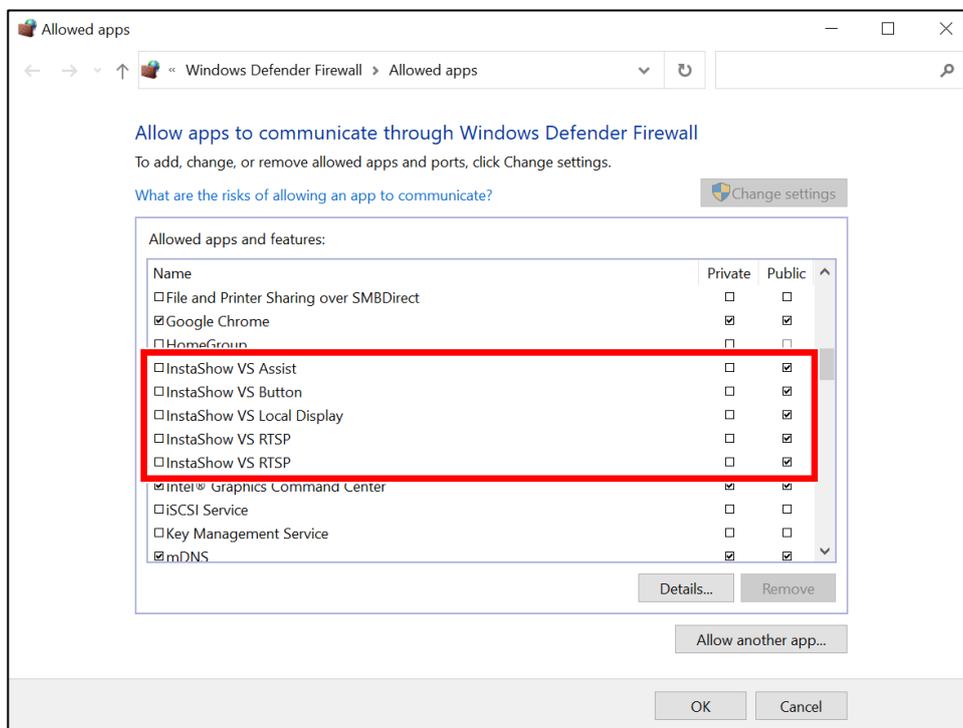


Figure 13: Windows Defender Firewall Allowed Apps

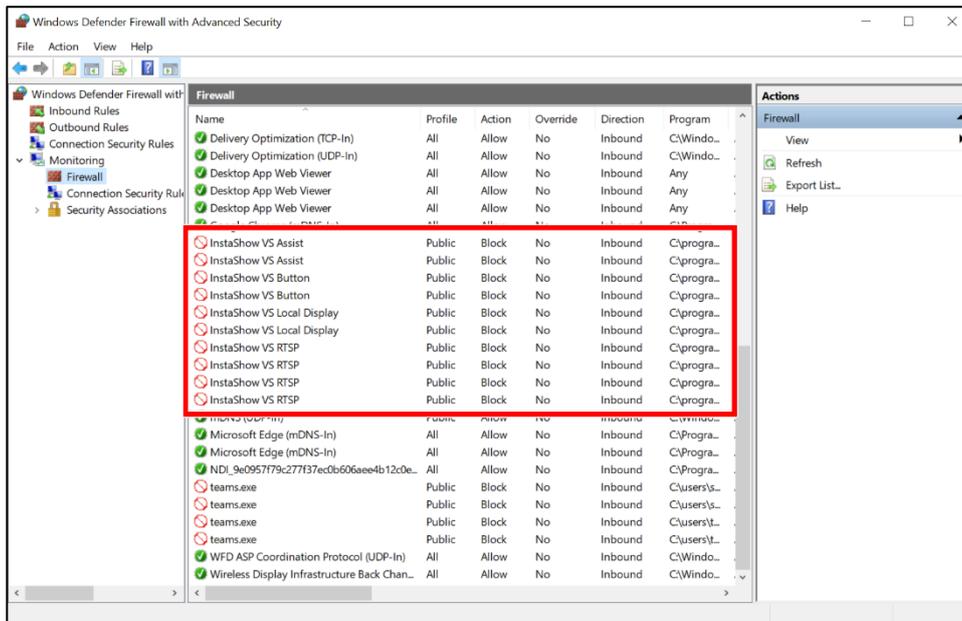


Figure 14: Windows Defender Firewall Advanced Security Menu

3.3 Network Switch/Routers and Cross Networks in a Corporate Network

Because of different network policies employed by different organizations, you should also remember to set up the organization's internal switches, routers, and firewalls to allow and forward the ports and packets discussed in this chapter through VLANs. If not, the video conferencing features for InstaShow VS20 may not function in your organization's network.

4 InstaShow VS Assist App Installation and Information

The InstaShow VS Assist app's .msi file contains the following packages which will be installed in the Windows operating system:

- VS Assist Main Application
- .NET Framework 5.0¹³
- InstaShow Virtual Drivers

4.1 Hardware Requirements for the InstaShow VS Assist App on a Windows PC

By installing the InstaShow VS Assist app on their PC a user will be able to connect their PC with the InstaShow VS20 Host and access the displays and video bars connected to the Host. Before installing the InstaShow VS Assist app, first ensure that your system meets the following minimum requirements:

- Memory: 8 GB RAM
- Hard Disk: At least 300 MB of available disk space
- Operating System: Windows 11 (64 bit)
- CPU: Intel Core i3 or an equivalent AMD processor

NOTE: For Intel processors, the maximum speed achieved during Intel Turbo Boost Technology (Max Turbo Frequency) must be considered.

4.2 Installing InstaShow VS Assist in a Corporate Environment

The InstaShow VS Assist app is released as an .msi file which is used as a Windows installer package for mass distribution to systems used by employees within an organization and can be run by certain Windows Command scripts generated by the IT staff. The .msi file must be installed by accounts with Administrator privilege.

¹³ The .NET Framework is a software development platform created by Microsoft that provides a programming model, a set of libraries, and a runtime environment for building and running applications on Windows-based operating systems. It includes a large class library, known as the Framework Class Library (FCL), and provides language interoperability across several programming languages.

Some organizations with strict IT policies might not allow employees to install new applications or related packages onto their system as the accounts used by their employees may be configured to Standard User settings without Administrator privileges (as seen in the figure below). Under such a policy, the installation or updating of applications and system packages will need to be done by IT staff.

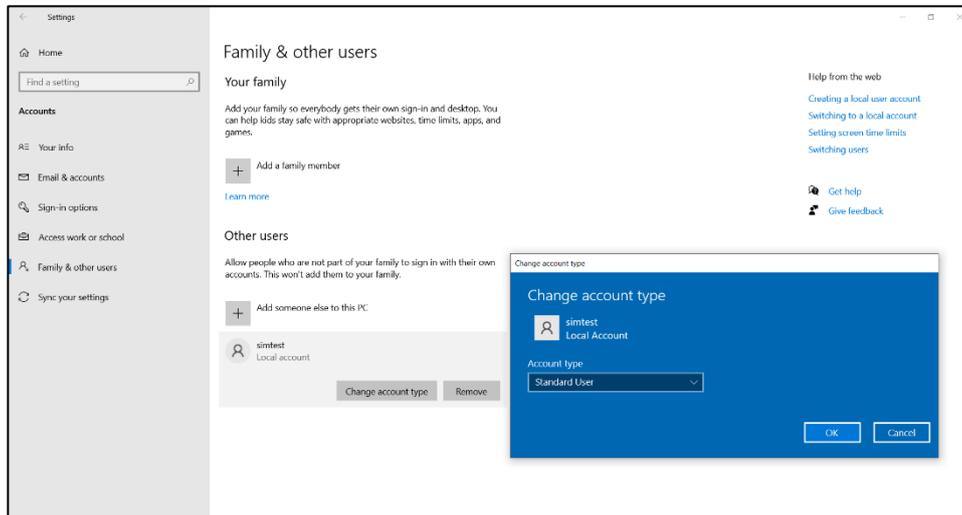


Figure 15: Windows Account Type for a Standard User

This article will not cover the steps used for mass deployment by IT staff but will instead only describe the standard full installation process for accounts with administrator privileges.

4.2.1 The Standard Full Installation Process

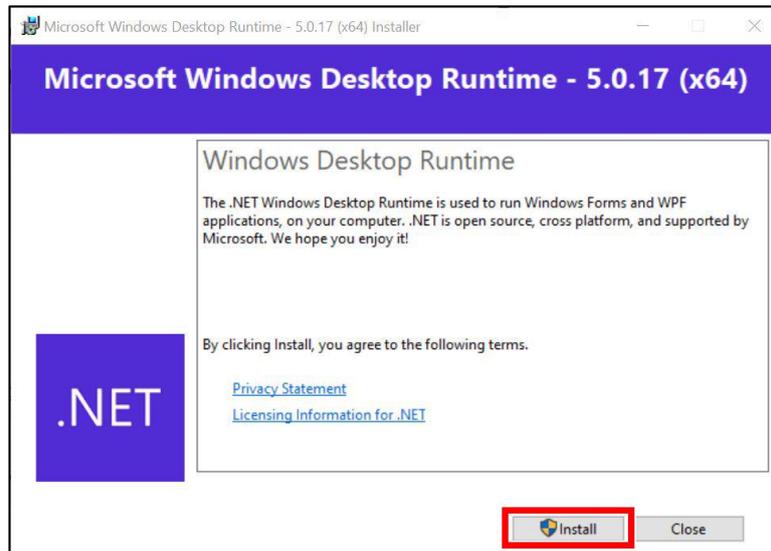
During the installation process, the InstaShow VS Assist app will check whether the system has already installed .NET Framework. If it has not already been installed, the application will display a pop-up asking you if you want to install it or not. You can skip .NET Framework installation if you want. If InstaShow VS Assist detects that .NET Framework has already been installed, it will skip its installation and proceed to install the InstaShow Virtual Drivers.

To utilize all the features of the main InstaShow VS Assist app, please install all three packages listed previously. If .NET Framework installation is skipped, the InstaShow VS Assist's presentation features will still work, but the app's **InstaShow Camera Preview** and **InstaShow Display Sharing** functions will not work.

To perform a standard full installation of the InstaShow VS Assist app for new users:

NOTE: When installing versions of the InstaShow VS Assist app higher than 1.0.0 on systems that have already installed version 1.0.0, you must first uninstall version 1.0.0 using Windows Uninstall prior to installing the newer version. This only needs to be done for systems with InstaShow VS Assist version 1.0.0.

1. Double-click the **InstaShow_VS_Assist_xxx.msi** file.
2. In the **Microsoft Windows Desktop Runtime** window, click **Install**. Let the installation proceed until finished.



3. Click **Close**.

The table below lists the functional differences between a fully installed application and an application that has skipped the .NET Framework installation.

Function	Full Installation	.NET Framework Installation Skipped
InstaShow VS Assist – Search	Yes	Yes
InstaShow VS Assist – Connect/Disconnect	Yes	Yes
InstaShow VS Assist – Camera Preview	Yes	No
InstaShow VS Assist – Display Sharing	Yes	No
InstaShow Virtual Driver for Video Conferencing	Yes	Yes

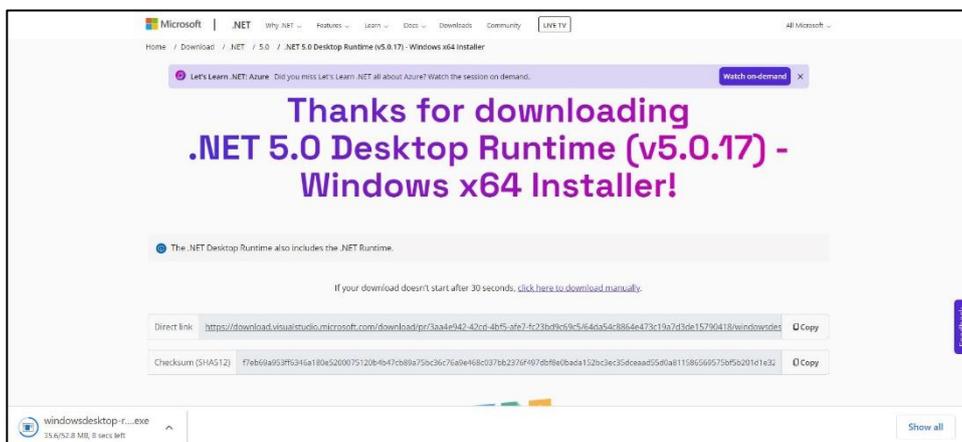
If you skipped the .NET Framework package installation but attempt to use the **InstaShow Camera Preview** and **InstaShow Display Sharing** functions within the InstaShow VS Assist app, Windows will allow you to choose whether to download and install it from Microsoft Office’s download site.

Follow the steps below to download and install the .NET Framework package:

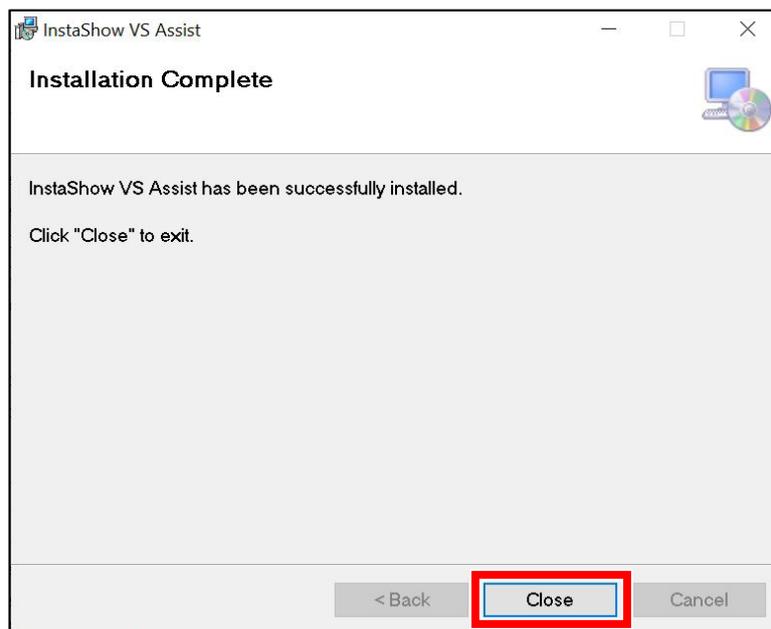
1. When a pop-up window appears notifying you to install .NET, click **Yes**.



2. Windows will forward you to the .NET Framework download page and begin automatically downloading the installation file. Once the download is finished install the .NET Framework package.

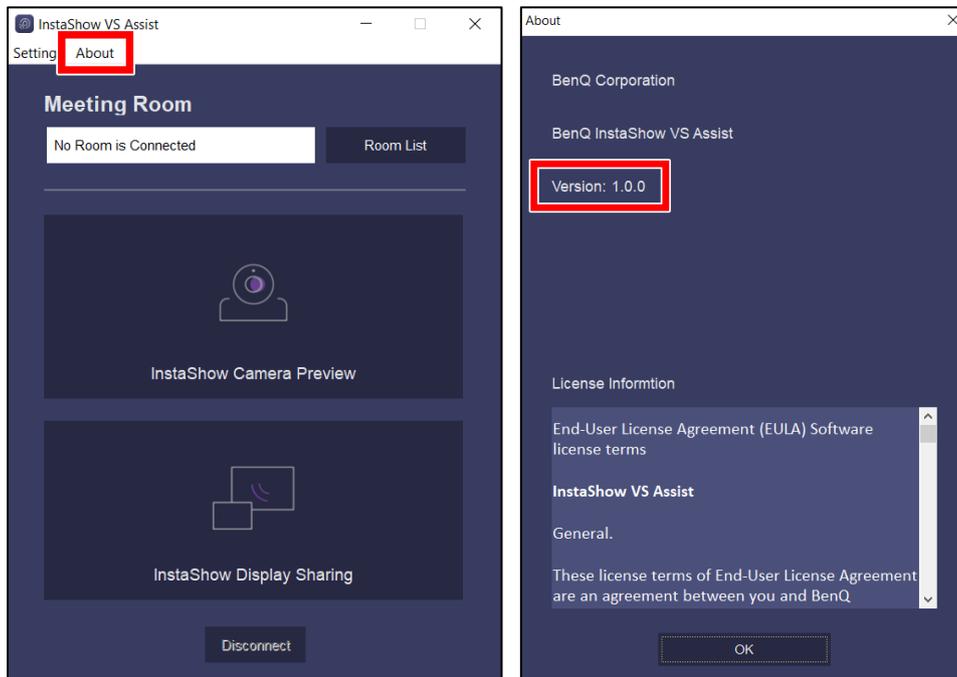


3. Once the installation is complete, click **Close** to finish the installation process.



Checking the InstaShow VS Assist Version

To check the InstaShow VS Assist app's version number, click **About** in the InstaShow VS Assist window and the version will be displayed in the resulting window.



5 Video Conferencing

5.1 Supported Video Conferencing Peripherals and Setup

Procedures

Below are the recommended installation procedures your organization’s IT staff can use to integrate USB video conferencing peripherals with InstaShow VS20.

5.1.1 About the InstaShow VS20 Host’s USB-A Ports

Because the USB-A 3.0 ports on the InstaShow VS20 Host are faster than its USB-A 2.0 port, it is recommended that you use the USB-A 2.0 port to connect touchscreen displays (if available) while reserving the USB-A 3.0 port for USB-A video conferencing peripherals for better performance.

NOTE: For peripherals that only feature USB-C connectors, please use a USB-C Female-to-USB-A 3.0 Male adapter to connect to the Host.

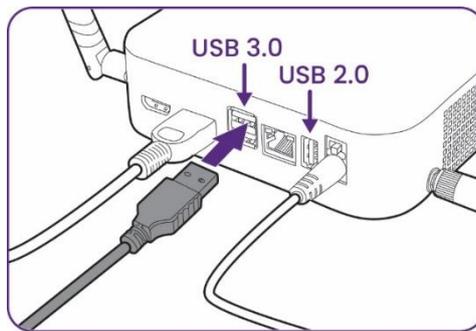


Figure 16: InstaShow VS20 Host's Rear USB-A Ports

Model Name	USB-A 3.0 Ports	USB-A 2.0 Ports
VS10	N/A	2
VS20	2	1

Table 8: Available USB-A Ports for InstaShow VS Series Models

The order of priority for the USB-A ports located at the rear of the InstaShow VS20 Host is as follows:

Model Name	Port Priority	Port Location
VS20	Port 1	Top USB-A 3.0 Port
	Port 2	Bottom USB-A 3.0 Port
	Port 3	USB 2.0 Port

Table 9: Order of Priority for USB-A Ports

Additionally, the InstaShow VS20 Host will also prioritize which connected peripheral devices will be used for each video conferencing function (microphone, camera, speaker) based on default settings. It's recommended that all-in-one video conferencing devices be set to the highest priority. For more information on manually setting device priorities, see Manually Selecting the Preferred Devices for a Specific USB-A Port on page 42.

When more than one speaker, microphone, or camera (including speakerphones and all-in-one cameras) are connected, only one of the devices will work for a corresponding function.

When two or more devices with the same function are connected (for example cameras connected to both USB-A 3.0 port), only the device connected to the top USB-A 3.0 port (Port 1) will work.

5.1.2 Connecting USB Peripherals to the InstaShow VS20 Host

InstaShow VS20 supports the following types of USB peripherals:

- Touchscreen displays with HID capabilities
- USB web cameras (support is for the camera feature only, InstaShow VS20 does not support the use of a USB web camera's built-in microphone)

NOTE: When using this type of USB peripheral, please use them in conjunction with the built-in microphones featured on InstaShow VS20 Buttons. Because the method for configuring this type of setup will vary based on the firmware version, please refer to the following webpage for the latest information:

<https://www.benq.com/en-us/business/support/faqs/before-sales/prj-prefaqs-00002.html>

- All-in-one video conferencing devices (camera, microphone, and speaker combo)
- Speakerphones (microphone and speaker combo)

Due to the variety of USB peripheral devices available on the market, it cannot be guaranteed that every single USB peripheral device is compatible with InstaShow VS20. BenQ InstaShow VS20 frequently updates its firmware to support new video conferencing devices, a list of which can be found on our website which you can link to [here](#).

Connecting peripherals to an external USB switch/hub and then connecting the switch/hub to the InstaShow VS20 Host's USB port is not recommended, because there may be power or compatibility issues between the Host and the switch/hub.

NOTE: Peripherals that are not listed on BenQ's website may still work with the InstaShow VS20 Host.

The figure below is a typical (wired) outline for InstaShow VS20 connections.

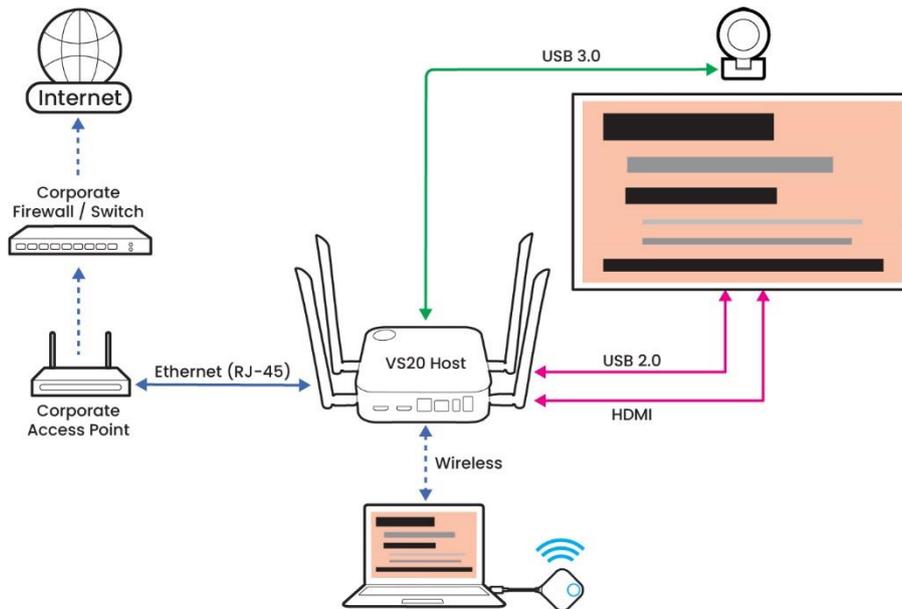


Figure 17: Typical Wired (Ethernet) Connection

Connecting only a single USB peripheral (i.e., all-in-one video conferencing devices) to the InstaShow VS20 Host is recommended to avoid conflicts between peripherals. When a separate web camera must be used, use it with a speakerphone (instead of two single devices via two separate USB-A ports). The following are additional rules and limitations for connecting USB peripherals:

- Separate microphones and speakers are not supported.
- Speakers and microphone must be incorporated in a single device (i.e., speakerphone)
- If a single web camera that is being used has a built-in microphone, only the camera feature is supported. Pair the web camera with a speakerphone in such a case.
- Connecting an all-in-one camera, video bar, or speakerphone, as opposed to connecting separate single-function devices, is the best method to connect peripherals.
- All audio output will be through a connected USB-A speaker instead of the HDMI output, as only one audio output path is supported.
- If a display with built-in speakers is connected via the HDMI output port, the speakers will NOT be supported in hybrid video conference scenarios.
- If a single speaker is connected to the VS20 host, the speaker will NOT be supported. Please always utilize speakerphones via a single USB-A 3.0 port (as opposed to two individual devices via two separate USA-A ports).

Standard Setup for an InstaShow VS20 Host and USB-A Peripherals

To set up USB peripherals with an InstaShow VS20 Host:

1. Connect the peripheral device's USB-A connector to one of the USB-A 3.0 ports at the rear of the Host.

NOTE 1: Only use the USB cable that was originally supplied with your peripheral as some cables are customized specifically for the peripheral and USB extension cables may cause power and data signal issues.

NOTE 2: Only use the power adapter that was originally supplied with your peripheral as the InstaShow VS20 Host only provides a standard USB power current (500mA for the USB-A 2.0 port; 900mA for the USB-A 3.0 ports). Insufficient power supply may cause unexpected issues.

NOTE 3: Only use high-quality USB-C to USB-A adapters if your peripheral only features a USB-C connector.

2. Power on the Host.

NOTE: Powering on the Host first and then connecting the peripherals or switching peripherals on the fly (while the Host is powered on) is NOT recommended.

3. Follow the instructions on the guide screen to download and install the InstaShow VS Assist app either directly from the Host or from BenQ's official download site.

NOTE: IT departments can mass deploy the InstaShow VS Assist app using a batch file instead of installing the app on company laptops one by one.

4. Launch the InstaShow VS Assist app.
5. Search for your meeting room and connect to the corresponding Host.
6. Open a video conferencing application and start a video conference and check to see if the corresponding function (camera, speaker, and/or microphone) for the peripheral works properly.

5.1.3 Using the InstaShow VS Assist App to Check the Compatibility of Connected USB Peripherals

The InstaShow VS Assist app provides a streaming connection between the InstaShow VS20 Host and the local PC hosting the video conference. Once the app has connected to the Host, the **InstaShow Camera Preview** function will be available for use.

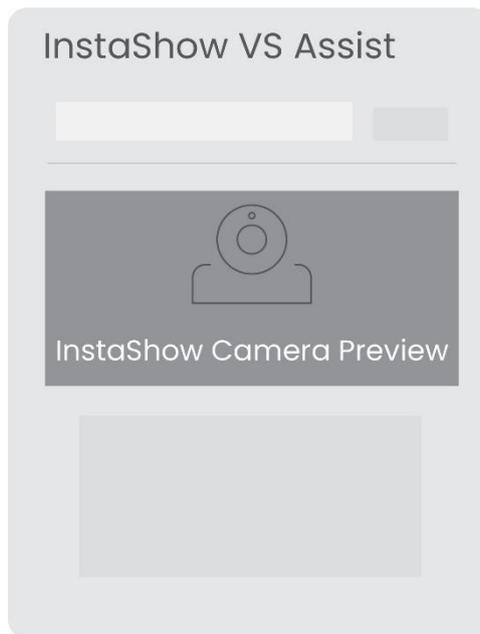
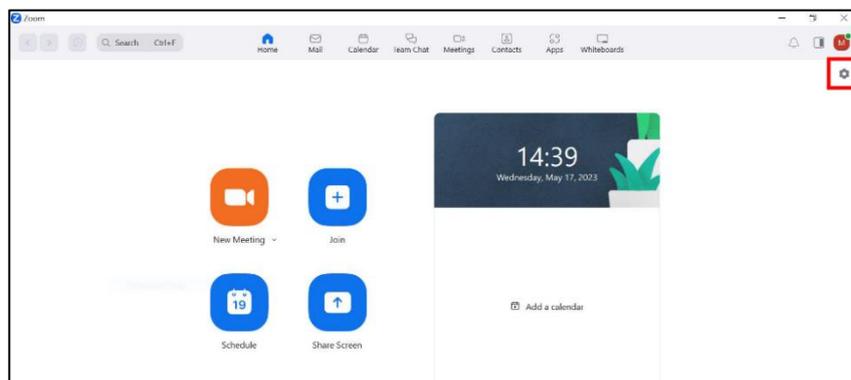


Figure 18: The InstaShow Camera Preview Button

The user can then click the **InstaShow Camera Preview** button within the app to check if the correct camera is being used. If the camera that is connected to the Host is not compatible with the InstaShow VS20, the **InstaShow Camera Preview** button will be unable for use.

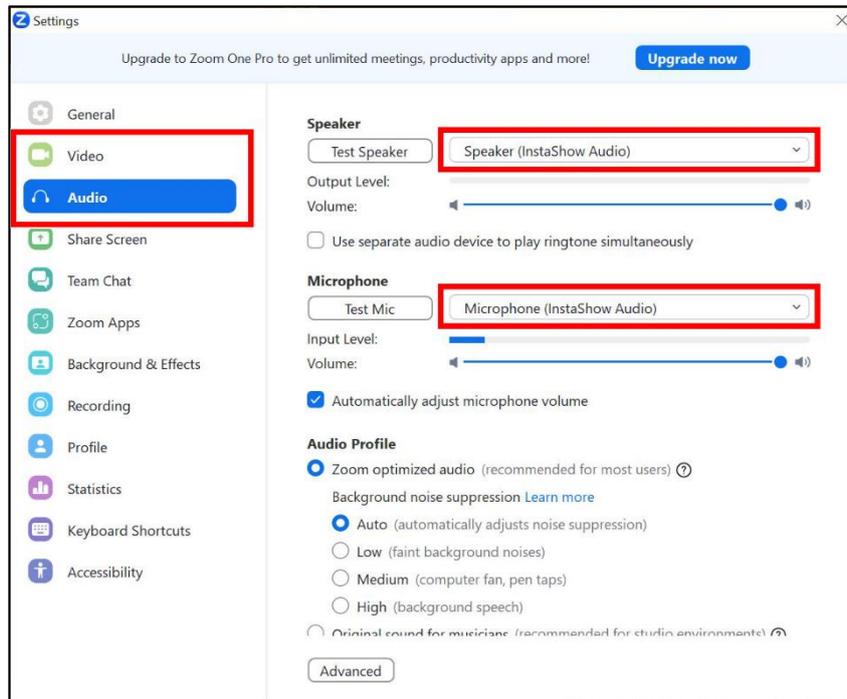
Another way to check if the camera and/or audio peripheral is working properly is via the video conferencing software, which is demonstrated below using Zoom as an example.

1. In the video conferencing software, click the settings button.



2. Choose one of the following to test a respective peripheral device:
 - For cameras: Select the **Video** menu and then select **InstaShow Camera** to check the camera stream.
 - For microphones: Select the **Audio** menu and then select **InstaShow Audio** in the drop-down menu. Click **Test Mic** to check the playback of a recorded sound clip.

- For speakers: Select the **Audio** menu and then select **InstaShow Audio** in the drop-down menu. Click **Test Speaker** to check the playback of a sample sound clip.



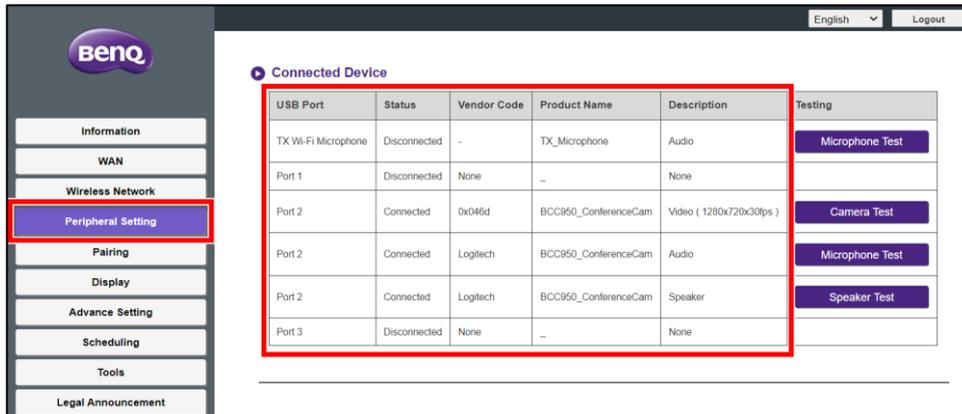
If none of the tests resulted in successful video/audio, follow the instructions in the next section to check the compatibility of the peripheral devices.

5.1.4 Using the Web Management Interface to Check the Compatibility of Connected USB Peripherals

The InstaShow VS20 Host's Web Management interface menu also features a tool that allows you to check the compatibility of a USB-A peripheral device connected to the Host.

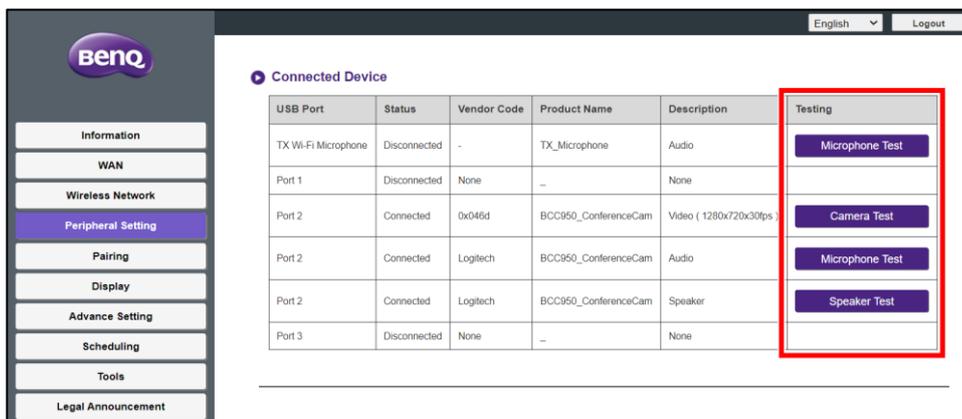
To check the compatibility of a peripheral device via the Web Management Interface:

1. Log into the Host's Web Management interface.¹⁴
2. Enter the **Peripheral Setting** menu.
3. Check the **Connected Device** table to see if the device information listed for the corresponding port is correct.



4. Click either **Camera Test**, **Microphone Test**, and/or **Speaker Test**, depending on the type of device you are using, to test the respective device.

NOTE: For a microphone test, the screen will turn blank for 5 seconds during which you should speak into the microphone, after the Host will playback the recorded sound. For the speaker test, a pulse sound will be broadcast by the connected speaker.



5.1.5 Manually Selecting the Preferred Devices for a Specific USB-A Port

By default, the InstaShow VS20 Host prioritizes which connected peripheral device to use per function in the following manner:

- All-in-one devices have the highest priority (i.e., will be used first as the device for each function)

¹⁴ Refer to the VS20 User Manual for instructions on logging into the Web Management interface.

First detected device based on the USB-A ports' order of priority detailed in Table 9: Order of Priority for USB-A Ports

These rules mean that if the InstaShow VS20 錯誤! 找不到參照來源。 Host detects that an all-in-one device is connected, it will use the device's camera, microphone, and speaker for each corresponding function. On the other hand, if two different devices with separate functions are detected, the first detected device (based on the order of priority for the USB-A ports) will be selected for use.

So, for an example of connections shown in the table below:

USB-A Port	Connected Device	Function(s)
Port 1 (Top USB-A 3.0 Port)	AverMedia PW513	Camera and Microphone
Port 2 (Bottom USB-A 3.0 Port)	Logitech BCC950	Camera, Microphone, and Speaker (All-in-one)

Table 10: Example Device Connection Matrix

The connection information in the **Connected Device** table of the **Peripheral Settings** menu will show what's displayed below:

NOTE: Each function for a device can be tested separately.

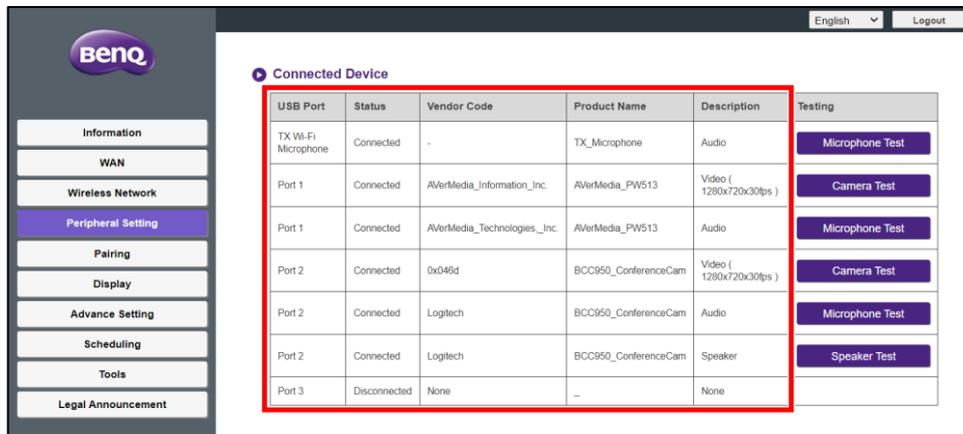


Figure 19: Example Connected Devices Table

The **VC Devices in Use** table in the **Peripheral Settings** menu will subsequently show the device used per function based on the logic described above. So, for the example described above, the **VC Devices in Use** table will show that the camera, microphone and speaker function are all set to the device connected to Port 2 (Logitech BCC950 All-in-One) because of the priority given to all-in-one devices.

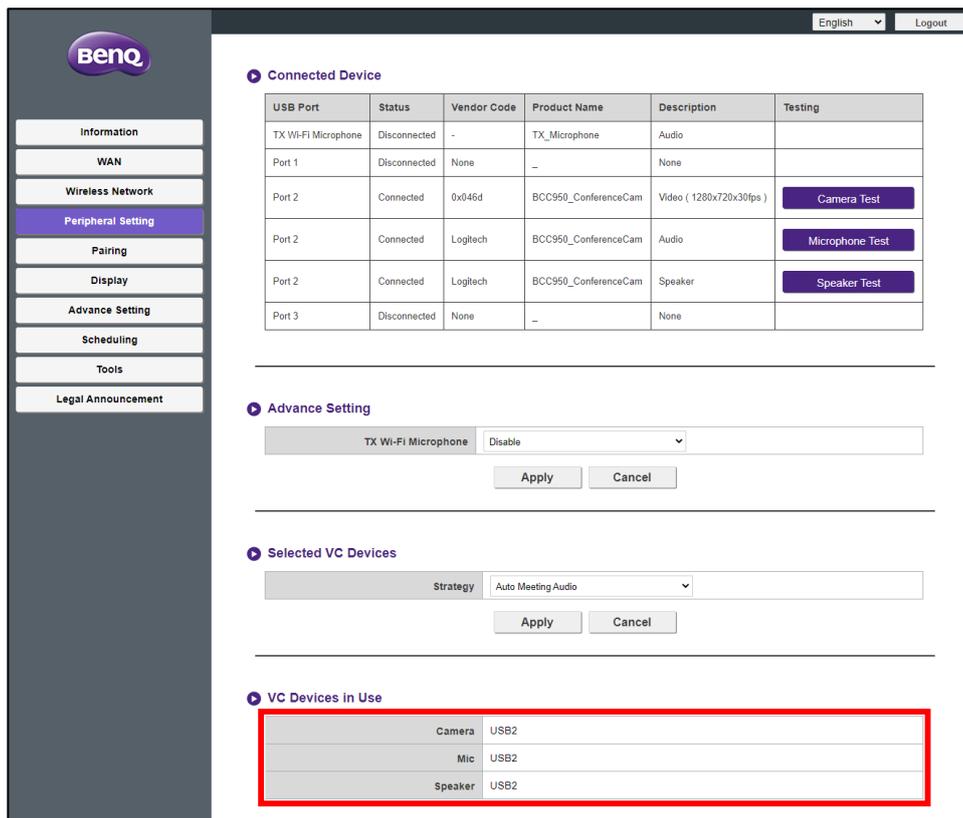
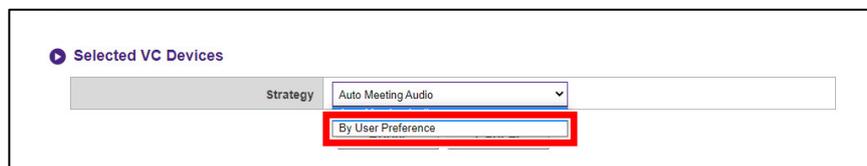


Figure 20: Example VC Devices in Use Table

If you want to forgo the default rules used to designate devices for video conferencing functions and manually set which device/port to use for a given function, follow the steps below:

1. Log into the Host's Web Management interface.¹⁵
2. Enter the **Peripheral Setting** menu.
3. In the **Selected VC Devices** sub-menu select **By User Preference** in the **Strategy** field. Additional rows for each video conferencing function (**Camera**, **Mic**, and **Speaker**) will then appear.



¹⁵ Refer to the VS20 User Manual for instructions on logging into the Web Management interface.

4. In the drop-down menu for each function, select the USB-A port for the corresponding device you want to designate for use.

Selected VC Devices	
Strategy	By User Preference
Camera	USB 1
Mic	USB 1
Speaker	USB 1

Apply Cancel

5. Click **Apply**.

Selected VC Devices	
Strategy	By User Preference
Camera	USB 1
Mic	USB 1
Speaker	USB 1

Apply Cancel

Echo Cancellation When Manually Selecting Devices

Because devices which feature both microphone and speaker functions tend to have Auto Echo Cancelling (AEC) and Auto Gain Control (AGC) capabilities, designating the microphone and speaker functions to different devices is not recommended, especially when speakerphones or all-in-one devices are available.

Please keep your firmware updated or go to our website [here](#) for the latest set up recommendations.

The wireless microphone feature for InstaShow VS20 will be discussed in another section. See also the Additional Notes section on page 51 for more related information.

5.1.6 Supported Camera Input Resolution and Codec

The InstaShow VS20 Host can support camera resolutions of up to 4K. For example, if you have a camera whose maximum resolution specification is 4K resolution, the Host will be able to support it. However, to ensure the widest compatibility for USB web cameras (given the variety of USB peripheral devices on the market and the various codec formats) while also taking into consideration optimal performance in a real-world environment, the InstaShow VS20 Host currently only supports the MJPEG codec and a maximum streaming resolution of 720p30fps when streaming via the InstaShow VS Assist app.

MJPEG is the most commonly supported codec for USB web cameras, but for the few cameras on the market that do not support MJPEG, the camera will not be compatible with the InstaShow VS20 Host. For details regarding supported resolutions and codecs, refer to the specifications provided by the camera manufacturer.

In terms of streaming resolution, 720p30fps is the most balanced optimal resolution suitable for a real-world environment. For cameras that do not support 720p30 resolution, the next selected resolution will be 1080p. However, this higher resolution will cause greater network bandwidth consumption.¹⁶

NOTE: Video conferencing applications will dynamically change the camera resolution, frame rate, and compression rate of the video feed in real time during a video conference based on the status of the network connection, meaning the video conference will not always be at the highest possible resolution, but instead will adjust the previous parameters to allow the video conference to proceed smoothly.

5.1.7 Default Audio Output

The default audio output for an InstaShow VS20 host for various connection scenarios is as follows:

Scenario	Default Audio Output Port/Device	Recommendation
Only HDMI connection (For example, when the built-in speakers on your HDMI display is the only audio output and no other USB-A device with a speaker function is connected)	HDMI Port	InstaShow VS20 does NOT support output to speakers via HDMI (see Connecting USB Peripherals to the InstaShow VS20 Host on page 37). Connect a speakerphone to the InstaShow VS20 Host's USB-A port.
One USB-A device with speaker function connected	USB-A	InstaShow VS20 does NOT support single-function speakers.
Two USB-A devices with speaker function connected	First USB-A device with speaker function detected (based on order of priority for Host's USB-A ports)	Connect a speakerphone or all-in-one video conferencing device to the InstaShow VS20 Host.

¹⁶ Users can refer to the specifications for their camera model provided by the manufacturer to check if their camera supports the MJPEG codec.

Table 11: Default Audio Output

The user can manually change the designated audio output using the steps described in the Manually Selecting the Preferred Mic Devices for a Specific USB-A Port section on page 42.

NOTE: Manually setting the audio output to a different device may cause echoing, especially if the device (speakerphone or all-in-one) has no built-in echo cancellation features.



5.2 Using InstaShow VS20 Buttons as Microphones

Each InstaShow VS20 Button features embedded microphones which allow them to be used as external wireless microphones for video conferences in a variety of ways, the guidelines of which will be detailed in this section.

5.2.1 General Introduction

When an InstaShow VS20 Button is plugged into a laptop, the operating system for the laptop (Windows for example) will automatically recognize it as a device in the **Audio inputs and outputs** list of its **Device Manager** menu, with a name **InstaShow Button Microphone**. This allows the Button to act as an omni-directional microphone that is able to pick up voices/sound within a 1.5-meter range in order to replace the typically weaker built-in microphone on the laptop itself.

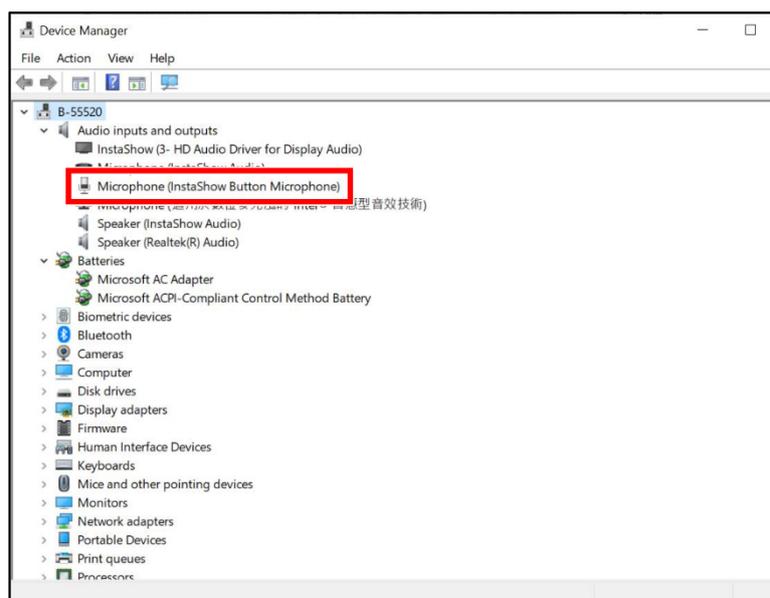


Figure 21: Windows Device Manager with InstaShow VS20 Button Connected

The InstaShow VS20 Button itself features a mute key which can mute/unmute any sound input from the Button's microphone.

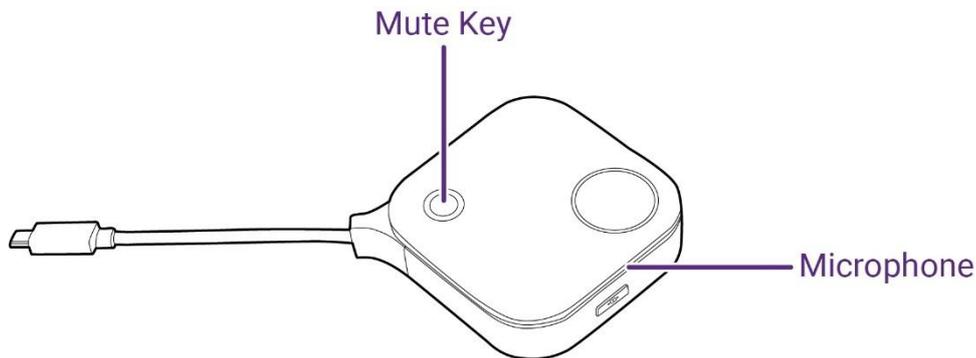


Figure 22: InstaShow VS20 Button

5.2.2 Using InstaShow VS20 as a Wireless Microphone System

Using an InstaShow VS20 Button as a microphone in tandem with an InstaShow VS20 Host allow users to create their own wireless microphone system.

Typical wireless microphone systems feature (1) a microphone receiver host and (2) microphone client transmitters that rely on a VHF/UHF or 2.4 GHz radio signal. The InstaShow VS20 Button on the other hand, utilizes a 5 GHz Wi-Fi signal as its transmission interface. Thus, the typical setup for an in-room wireless microphone system will include the following:

- An LCD display
- A central control system
- An audio mixer
- Microphones
- An Amplifier
- Speakers

A wireless microphone system formed out of an InstaShow VS20 Host and Buttons is geared more towards video conferences while simultaneously being able to be integrated with existing in-room systems. With an InstaShow VS20 wireless microphone system, the Host then acts as the microphone receiver host and the Buttons act as the microphone transmitters. The Host then aggregates the audio signals from all the transmitters, including any external microphones connected to the Host's USB-A port, and outputs to remote participants via the InstaShow VS Assist app and the video conferencing application installed on the host PC for the meeting.

The following is the recommended microphone deployment plan for an InstaShow VS20 system based on conference room type/size:

Room Type/Size	Microphones to Use	Additional Recommendations
Small	InstaShow VS20 Button Microphone <i>or</i> USB-A Peripheral Device	Enable only a single microphone as the audio input source
Medium (Square)		
Medium (Rectangular)	InstaShow VS20 Button Microphone <i>and</i> USB-A Peripheral Device	Enable both types of microphones as the audio input source to aggregate sound
Large (Conference/Board Room)		
Large (Auditorium / Multipurpose Room)		

Table 12: Recommended Microphone Deployment

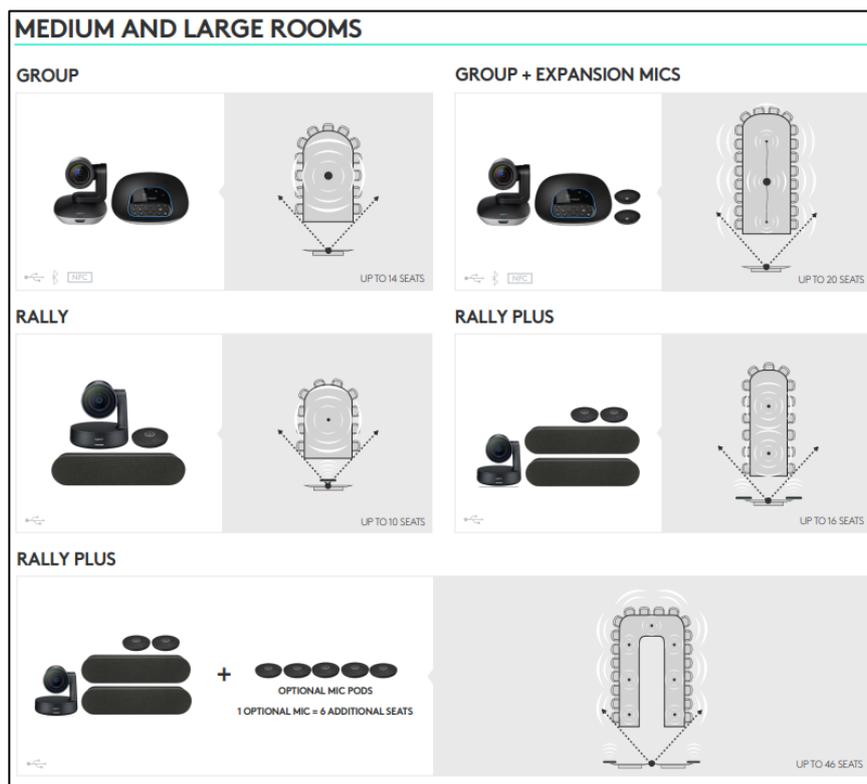
The most suitable use of InstaShow VS20 Buttons as microphones during a video conferencing scenario is when the connected USB peripheral with microphone capabilities has a limited range.



Figure 23: Example Meeting Room

For instance, in the example above the medium-sized meeting room features a USB peripheral microphone (Logitech BCC950¹⁷) that has a range of 2.4 meters. While the recommendations for the peripheral model used suggests adding expansion microphones from the same brand to increase coverage for the room, budget limitations and/or model availability might prevent the organization from being able to purchase any. Yet because of its 2.4-meter range, the organization will still need to find a way to expand the range of the USB peripheral they already have on hand. The availability of InstaShow VS20 Buttons allows the organization to use them instead as expansion microphones to complement the existing USB microphone and fully cover the room.

Consequently, in the actual device suggestions provided by Logitech for various room layouts seen below, the wireless microphone client transmitters can be replaced by InstaShow VS20 Buttons. Each resulting setup would allow the InstaShow VS20 Host to aggregate the sound from the USB peripheral and each Button with no additional configurations, and then broadcast it to the video conference via the InstaShow VS Assist app.



¹⁷ For more information on Logitech BCC950, refer to the official product page: <https://www.logitech.com/en-in/products/video-conferencing/conference-cameras/bcc950-conferencecam.960-000939.html>

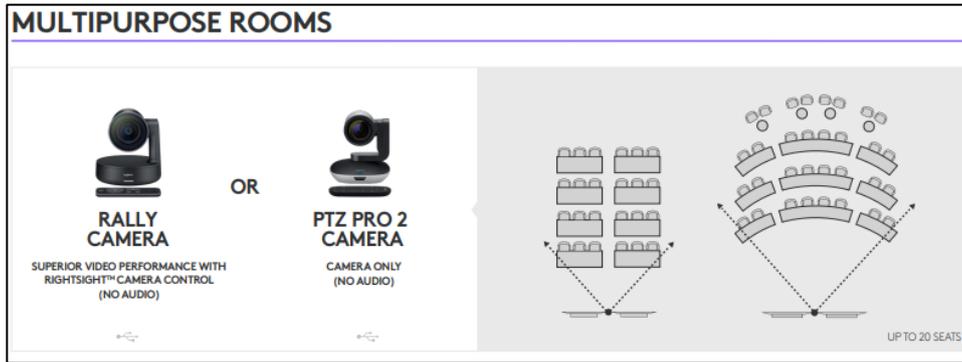


Figure 24: Device Suggestions from Logitech¹⁸

5.2.3 Setting Up an Aggregated Wireless Microphone System with InstaShow VS20

By default, the wireless microphone feature for InstaShow VS20 Buttons is enabled so that the sound from all connected Buttons will be aggregated with the sound from any USB peripheral with microphone capabilities connected to the InstaShow VS20 Host. As a result, users do not need to manually enable this feature.

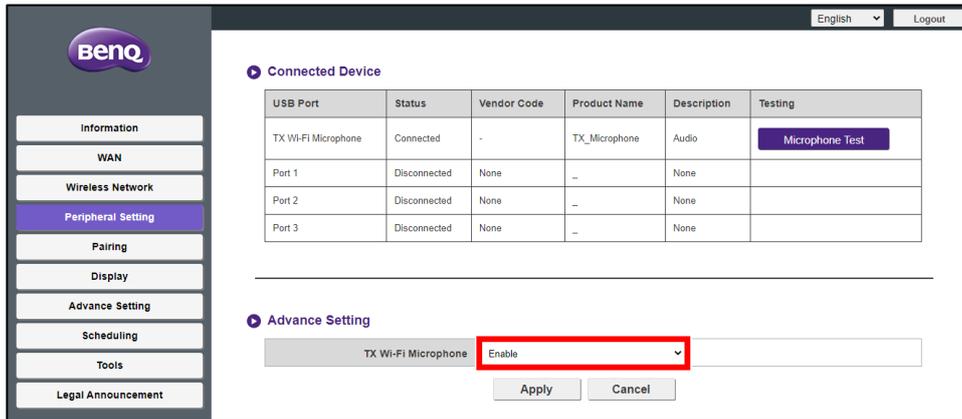


Figure 25: Wireless Microphone Enabled in Web Management Interface

Additional Notes

Because the microphone on each InstaShow VS20 Button is omni-directional and has a range of 1.5 meters, interference may occur in certain instances. The cause of interference generally falls under two categories:

- Wireless Interference
- Voice Interference

¹⁸ The device suggestions shown can be downloaded from Logitech's website: <https://www.logitech.com/content/dam/logitech/en/video-collaboration/pdf/logitech-fov-diagram-web.pdf>

Wireless interference usually occurs when the wireless environment or channel is too busy, thus it is recommended you follow the recommendations in Chapter 2: “Installing VS20 into your Network Configuration” before setting up the InstaShow VS20 Host to minimize interference.

Voice interference can come in two forms: (1) echoes from remote or local participants, or (2) reverb for remote participants. To avoid echoes and/or reverb:

- Do NOT let multiple InstaShow VS20 Buttons come too close to one another. It’s best to use each Button 1.5 meters apart, so if echoes or reverb occur, increase the distance between each button.
- Use all-in-one video conferencing devices or speakerphones with AEC capabilities. Do NOT use separate microphones and speakers.
- In cases where you have a webcam with video and microphone capabilities only, but do not have a peripheral speaker connected, keep the webcam away from the actual equipment broadcasting the sound (i.e., a speaker system or the display).
- Keep your firmware updated and/or follow the instructions on our website [here](#).

If echoes and reverb still occur despite all the precautions taken above, take the following actions:

- Disable the wireless microphone feature via the **TX Wi-Fi Microphone** field in the **Peripheral Setting** menu of the InstaShow VS20 Host’s Web Management Interface and ensure that only the USB peripheral connected to the Host is used for the microphone function.

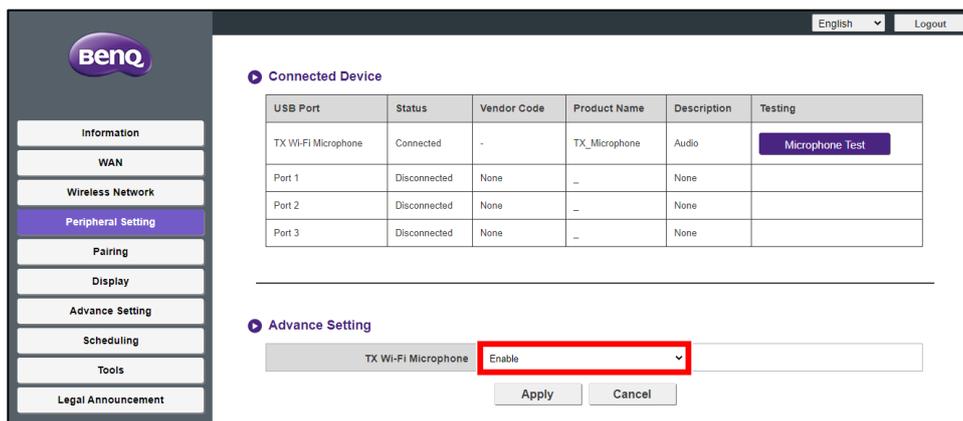


Figure 26: The TX Wi-Fi Microphone Field

- Mute the USB peripheral with the microphone capabilities and use only the InstaShow VS20 Button(s) as the microphone.

Some devices may have compatibility issues with the InstaShow VS20 Host when used as a wireless microphone system, thus it is strongly recommended that you use only devices that are recognized by BenQ as being compatible with InstaShow VS20, a list of which can be found on our website.

NOTE: InstaShow VS20 Host does not feature AEC or ANS capabilities when using InstaShow VS20 Buttons as wireless microphones. It only supports AGC capabilities.